CN1281561A Waveform and frame structure for fixed wireless loop synchronous CDMA communications system

Bibliography

DWPI Title

Waveform and frame structure for fixed wireless loop synchronous CDMA communications system

English Title

Waveform and frame structure for fixed wireless loop synchronous CDMA communications system

Assignee/Applicant

Standardized: **L 3 COMM CORP**

Inventor

STEPHENSON P L ; GIALLORENZI T R ; HARRIS J M

Publication Date (Kind Code)

2001-01-24 (A)

Application Number / Date

CN1998812005A / 1998-11-16

Priority Number / Date / Country

US1997988026A / 1997-12-10 / US
CN1998812005A / 1998-11-16 / CN

Abstract

[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
G06F 11/10
H04J 3/24 H04L 1/02
H04B 15/00 H04K 1/00

[12]发明专利申请公开说明书

[21]申请号 98812005.4

[43]公开日 2001年1月24日

[11]公开号 CN 1281561A

[22]申请日 1998.11.16 [21]申请号 98812005.4
[30]优先权
[32]1997.12.10 [33]US [31]08/988,026
[86]国际申请 PCT/US98/24472 1998.11.16
[87]国际公布 WO99/30234 英 1999.6.17
[85]进入国家阶段日期 2000.6.9
[71]申请人 L-3通讯公司
地址 美国纽约州
[72]发明人 P·L·斯蒂芬森 T·R·吉尔洛伦兹
J·M·哈里斯 L·A·布特菲尔德
M·J·胡尔斯特 D·格里芬
R·汤普森

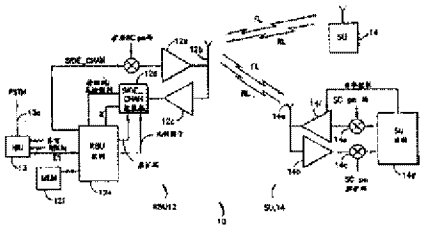
[74]专利代理机构 中国专利代理(香港)有限公司
代理人 邹光新 王忠忠

权利要求书2页 说明书10页 附图页数5页

[54]发明名称 固定无线环路同步CDMA通信系统的波形和帧结构

[57]摘要

公开了一种方法,用于在CDMA通信系统里发射信息,包括(a)将数据和控制信息复合(53)成一个数据流;(b)对这一数据流编码(54),形成编码I/Q码元对构成的一个流(62A、62B);(c)将同步信息插入这一编码I/Q码元对形成的流;和(d)作为一帧发射之前,用同样的伪噪声(pn)扩频码(14e)将这一编码I/Q码元对和插入的同步信息扩频。最佳帧结构包括一个未编码的同步字段,其后是多个多字节数据字段。这多个数据字段(80A)中的每一个都被控制消息字段(80B)隔开。控制消息字段中的每一个都包括多字节控制消息帧(82)中的一个字节。



ISSN1008-4274

00.06.09

权 利 要 求 书

1.在码分多址通信系统里发射信息的一种方法，包括以下步骤：

将数据和控制信息复用到一个数据流里；

对这一数据流编码，形成编码 I/Q 码元对组成的流；

在上述编码 I/Q 码元对形成的流里插入同步信息；和

在作为帧发射之前，用同样的伪噪声（pn）扩频码对编码 I/Q 码元对和插入的同步信息扩频。

2.权利要求 1 的方法，其中的复合步骤产生了一个数据流，该数据流的数据字段包括控制消息字段隔开的多个数据字节，每一个控制消息字段都包括一个字节的控制消息帧。

3.权利要求 2 的方法，其中的控制消息帧包括一个控制消息报头字段、多个控制数据字段和多个数据完整性字段。

4.权利要求 1 的方法，其中的帧包括一个未编码同步字段，其后是每一个都有多个数据字节的多个数据字段，这多个数据字段中的每一个数据字段都被控制消息字段隔开，每一个控制消息字段都是多字节控制消息帧的一个字节。

5.权利要求 1 的方法，其中的编码步骤包括以下步骤：

对数据流进行 1/2 速率卷积编码，产生 I 信道和 Q 信道信号；和

对 I 和 Q 信道进行 4/5 速率收缩栅格编码。

6.在码分多址通信系统里发射信息的一种方法，包括以下步骤：

将数据和控制信息复用到一个数据帧，数据帧的数据字段包括多个数据字节，这些数据字节被控制消息字段隔开，每一个控制消息字段都包括多字节控制消息帧的一个字节；

对这一数据帧编码；

用一个未编码同步字段插入这一数据帧；

用扩频码对数据帧扩频；和

将扩频数据帧发射给接收机。

7.权利要求 6 的方法，还包括以下步骤：

接收发射的数据帧并解扩；

跟同步字段同步；

对数据帧译码；和

分离控制消息字段和数据字段。

8.权利要求 7 的方法，其中的控制消息帧包括一个控制消息报头字段、多个控制数据字段和多个数据完整性字段。

9.权利要求 6 的方法，其中的编码步骤包括以下步骤：

对这些数据帧进行 1/2 速率卷积编码，产生一个 I 信道和一个 Q 信道；和

对 I 和 Q 信道进行 4/5 速率收缩栅格编码。

10.一种同步 CDMA 固定无线系统，包括一个无线电基站单元（RBU），跟电信网和多个用户单元（SU）相连，用 CDMA 无线电信道通信，该 RBU 包括：

第一个复用器，将给 SU 的数据和控制信息复用到一个数据帧，数据帧的数据字段包括控制消息字段隔开的多个数据字节，每一个控制消息字段都包括多字节控制消息帧的一个字节；

一个编码器，对上述数据帧编码，形成编码 I/Q 码元对；

第二个复用器，将同步字段的未编码 I/Q 码元对插入编码 I/Q 码元对，形成复用 I/Q 码元对流；

一个扩频器，用一个 pn 扩频码对上述复用 I/Q 码元对流扩频；和

一个发射机，将上述扩频复用 I/Q 码元对流作为一帧发射给目标 SU。

11.权利要求 10 的系统，其中的编码器包括：

一个 1/2 速率卷积编码器；和

一个 4/5 速率收缩栅格编码器。

12.权利要求 10 的系统，其中发射的帧包括一个未编码同步字段，其后是多个数据字段，每一个字段都包括多个数据字节，这多个数据字段中的每一个都被控制消息字段隔开，每一个控制消息字段都包括一个多字节控制消息帧的一个字节。

说　明　书

固定无线环路同步 CDMA 通信系统的波形和帧结构

发明领域

笼统而言，本发明涉及无线本地环系统，具体而言，涉及在无线电基站单元和多个用户台之间提供语音和数据通信的固定无线环路系统。

发明背景

本地环的传统定义是网络里将用户的家跟中心局交换机连接的那部分。然而，这是一个扩展的定义，当网络通过数字环路载波和数字交叉连接扩展到本地环时，情况并非如此。在本发明中，本地环指的是从用户住宅到网络连接点的连接，而不管这种连接是用什么方式实现的。

直到最近，本地环主要采用铜线，对于遥远的区域或者崎岖的地形，就用微波无线电链路来补充。最近十年里，光纤进入了本地环（也叫做“接入”网）领域，离用户的家和建筑更近了。基于 sonet 的接入网把光纤拉到了路边。这些光纤可以在商业用户非常稠密的市区/大城市非常可靠、非常经济地提供宽带业务。事实上，美国的多数接入提供商都采用这种基于光纤的设备，为美国的商业用户提供接入业务。

尽管铜线和光纤方案在许多场合里都非常经济，但它们仍然有许多缺点。

例如，在没有现成网络基础设施的地区，建设新网络非常耗时，成本也很高。成本主要在于劳动力、权利的获得（获得通行权或者地役权）以及电子学（对于光纤接入）。总的说来，这一过程非常缓慢，因为获得通行权并完成必须的建设，包括空中和/或地下的，需要艰苦的努力。还有，在已经挤满了电缆的地方，提高容量是非常昂贵的，因为已经布满了管道和电缆，有时不对整个系统重新分类和升级，根本无法提高容量。另外，有线方式的成本跟距离很有关系，因此，在人烟稀少的地区，不适合使用。有线网还很难重新铺设，当需要（用户）转移时，会造成财产的损失。在紧急情况下，还无法迅速地铺设有线网。

术语“固定无线环路”，也就是 FWL，指的是基于无线方式的本地接入。但是，它经常跟用更一般性的术语“无线电接入”表示的有有限移动性的解决方案混淆起来。跟采用哪种无线电技术无关，所有的固定无线或者无线电接入系统都使用无线方式为用户提供网络接入。一般而言，有三种固定无线方式。

固定蜂窝系统的主要基础是现有的模拟蜂窝系统，例如 AMPS（在北美）或者 NMT（在北欧国家）。

固定无绳系统的主要基础是采用数字 TDMA 时分双工技术的欧洲 DECT 标准。

定制系统（bespoke systems）是专门为固定无线应用设计的。这种传统的系统是模拟方式的点到多点系统。新近开发的系统采用更高的频率和数字技术。这些系统可以用相似的蜂窝技术来导出，但不是基于任何现成的大家都认可的标准上的。

在这三种主要的固定无线系统里，没有一种明显比另一种更好。如果对系统操作员的主要要求是提供语音业务，其中的语音质量不是一个限制因素，那么，固定蜂窝系统常常就很合适，甚至是必需的，因为它的设备成本相对较低。对于人口密集的市区，可能需要 DECT 方式，因为它的容量较大，并采用了皮蜂窝方式。对于人口稀疏的地区，微波是最佳方案。定制系统在许多情况下都很合适，总质量最好，功能也完善，但它们很可能更贵，至少在最近的将来仍然是如此。

经济欠发达地区的多数住宅用户其主要兴趣在于合适的语音业务。但多数商业用户除了语音以外，还需要数据和传真业务。随着家用计算机和因特网接入的迅速普及，需要为住宅用户提供高速数据业务。因而总的趋势是，所有的用户，包括住宅用户和商业用户，都希望获得高质量的语音和数据业务。

传统码分多址通信系统的问题是系统的容量受限于有限的伪噪声（pn）扩频码个数。在一个信道里采用两个 pn 码对同相（I）和正交（Q）码元对扩频（和解扩）时，这一问题更加复杂。

传统通信系统的另一个难题涉及发射控制消息。通常是将控制消息放进一个队列里以便尽早地发射出去，帧结构一般都被设计成在帧头或帧尾发射在一块中的一个特定帧的所有控制消息。然而，为了在帧头或者帧尾为一块中的一个特定帧发射所有的控制消息，这一方法

会带来延迟。例如，如果有一个字节的消息在队列的顶部，这时碰巧一帧刚刚结束，这一消息就必须等待整整一帧的时间，直到下一块准备好以后才能发射出去。在这种情况下，这一延迟相当于整整一帧。

发明目的和优点

因此，本发明的第一个目的和优点是提供一种改进了的固定无线环路系统，它能满足前面介绍过的需求以及其它的需求。

本发明的另一个目的和优点是提供一种改进了的固定无线环路系统，它改进了 pn 码的使用，还解决了控制消息的延迟难题。

发明简述

上述问题和其它问题，上述目的和优点，是用本发明的实施方案里的方法和装置来解决和实现的。

这里公开的是一种方法，用于在 CDMA 通信系统里发射信息，该方法包括（a）将数据和控制信息复用成一个数据流；（b）对数据流编码，形成编码 I/Q 码元对构成的流；（c）在这一编码 I/Q 码元对构成的流里插入同步信息；以及（d）作为一帧发射之前，用同样的伪噪声（pn）扩频码对编码 I/Q 码元对和插入的同步信息扩频。

多路复用步骤产生了有许多数据字段的一个数据流，这些数据字段包括多个数据字节，用控制消息字段分开，每一个字段都包括控制消息帧的一个字节。这一控制消息帧包括一个控制消息报头字段、多个控制数据字段和多个数据完整性字段（data integrity fields）。

更具体地说，这一帧包括一个未编码同步字段，后面紧跟多个数据字段，每一个字段都包括多个数据字节。这多个数据字段中的每一个都用一个控制消息字段分开。所有的控制消息字段都包括多字节控制消息帧的一个字节。

在本发明的优选实施方案里，编码步骤包括（a）对数据流进行 1/2 速率卷积编码，产生一个 I 信道和一个 Q 信道；和（b）对 I 和 Q 信道进行 4/5 速率收缩（punctured）栅格编码。

附图简述

在以下说明中，通过参考附图，本发明的上述特征和其它特征将更加显而易见。在这些附图中：

图 1 是本发明中同步 DS-CDMA 固定无线通信系统的一个简化框图，该系统有一个无线电基站单元（RBU）和多个收发信机或者用户

单元（SU）. RBU 向 SU 发送边信道（side channel）信号，并从这些 SU 接收基本上是异步发射的边信道信号。

图 2 是图 1 所示系统的频率分配图实例。

图 3 是更详细地说明图 1 所示 RBU 和 SU 的框图。

图 4 是当前的优选帧结构，其中的数据字段用控制消息帧字段隔开。

图 5A 和 5B 更详细地分别说明 RBU 发射和接收电路。

发明详述

通过介绍，并参考图 1 可以看出，本发明一个优选实施方案中的固定无线系统（FWS）10 是一种基于数字无线电技术的定制系统。具体而言，FWS 10 通过空中链路采用基于直接序列扩频的 CDMA 技术，为用户提供本地接入。它质量很好，可靠性很高，成本又可以跟有线方式一争高低。FWS 10 频谱效率很高，因此，可以用有限的带宽提供很好的有线质量的业务。FWS 10 具有很大的动态范围，使得它能够用于皮、微或者迷你（mini）蜂窝体系结构，满足人口稠密的大城市、市区和市郊群体的需求，同时又非常经济。

FWS 10 的一些重要特性包括：以 32 kbps 速率传输的有线语音质量；32 kbps 速率的数据和传真吞吐量；很高的业务可靠性和很好的抗干扰性能；安全的空中链路；并支持增强型业务，例如入站和出站优先级/紧急呼叫。

FWS 10 的容量比传统异步 CDMA 技术高三到五倍，比当前时分多址（TDMA）技术的容量高三到七倍，原因是它能够实现频率复用。

FWS 10 是一种同步 CDMA（S-CDMA）通信系统，其中从无线电基站单元（RBU）12 到多个收发信机单元，这里叫做用户单元（SU）14，的正向链路（FL）上发射的是时间上对齐的码元和码片，其中的 SU 14 用于接收 FL 信号，并实现同步。所有的 SU 14 还要在反向链路（RL）上发射信号给 RBU 12，以便使它发射给 RBU 12 的信号实现时间同步，并一般性地实现双向通信。FWS 10 适合用于在 RBU 12 和 SU 14 之间实现传递语音和/或数据的电信系统。

SU 14 构成用户住宅设备（CPE）的一部分。CPE 还包括一个网络终端单元（NTU）和一个不间断电源（UPS），图 1 里没有画出。

RBU 12 包括产生多个用户信号（用户 1~用户 n）的电路，图 1 里

没有画出；还包括一个连续发射的同步边信道（SIDE_CHAN）信号。这些信号都分配了一个对应的 pn 扩频码，将它们传送给有一付天线 12b 的发射机 12a 之前，要对它们进行调制。在 FL 里发射时，采用的是相位正交调制，并假定 SU 14 都包括合适的相位解调器，以便从中获得同相（I）和正交（Q）分量。RBU 12 能够在多个频道里发射信号。例如，每一个频道都包括多达 128 个码信道（code channel），其中心频率的范围是 2~3 GHz。

RBU 12 还包括一个接收机 12c，接收机 12c 的输出跟边信道接收机 12d 连接。这一边信道接收机 12d 接收接收机 12c 的扩频信号、比例因子信号和边信道接扩 pn 码作为输入。这后两个信号来自 RBU 处理器或者控制器 12e。比例因子信号可以是固定的，或者可以是在反向信道里发射信号的 SU 14 的个数的函数。边信道接收机 12d 输出一个检测到/未检测到信号给 RBU 控制器 12e，用来说明是否检测到有一个 SU 14 正在发射信号，并输出一个功率估计值χ，如下文所示。读/写存储器（MEM）12f 跟 RBU 控制器 12e 有一个双向连接，用于储存系统参数和其它信息，例如 SU 定时相位信息和功率估计值。

网络接口单元（NIU）13 通过适合于本地公用网的模拟或者数字干线，将 RBU 12 跟公用网连接起来，例如公共交换电话网（PSTN）13a。RBU 12 用 E1 干线跟 NIU 13 连接，用同轴电缆跟它的主天线 12b 连接。SU 14 通过上述无线电接口跟 RBU 12 通信。

另外，FWS 10 还有一个基本管理系统，也就是 EMS（没有画出），它为 NIU 13 和 RBU 12 提供操作、管理、维护和供应（OAM&P）功能。EMS 的功能对于理解本发明并不是至关重要的，因此不予详细介绍。

NIU 13 是系统 10 跟公用网的接口。它的主要用途是提供公用网所需要的专用协议和信令。这些协议可能随着国家的不同而不同，也可能随着用户的不同而不同，甚至有可能随着网络内连接点的不同而不同。

在本发明的一个优选实施方案里，NIU 13 可以跟最多 15 个 RBU 12 连接，每一个 RBU 12 用 1 到 4 个 E1 连接，人口稠密的地方 RBU 12 用 4 个 E1 连接。另外，每一个 NIU 13 都可以容纳例如 10000 个用户。所有 E1 干线的时隙 16 都用于在 NIU 13 和连接的 RBU 12 之间传递控

制信息，以及跟控制 EMS 交换信息。这一协议是基于 HDLC 格式的，为强化 RBU-NIU 通信而进行了优化。

NIU 13 提供的具体功能包括：RBU 12 的初始化；提供拨号音和 DTMF 信号给 SU 14；建立和拆除语音和数据呼叫；维护呼叫详情记录（CDR）数据；HDLC 协议（到 RBU 链路控制处理器的数据链路协议）；计费系统接口；用于振铃和摘机/挂机检测的公用信道信令（CCS）；在 NIU、RBU 和 SU 里检测双占用；呼叫优先级管理；为进行中的呼叫重新分配信道；检测拍叉簧信号以支持普通老式电话业务（POTS）和增强型 POTS 呼叫功能；32/64 kbps 速率变换的初始化；投币式公用电话功能（12/16 kHz 音频信号检测、线路反接；优先级和紧急号码呼叫；支持国家专用信令接口，例如 E&M、R1、R2、R2 变量和 C7；以及系统模块化：线路侧和干线侧的模拟/数字选择。

SU 14 的正常工作模式是使用符合 ITU-T G.721 标准的 ADPCM 编码方式的压缩语音模式。这一长话质量（toll quality）的 32 kbps 业务是 RBU 12 建立了非 X.21 信道的情况下使用的默认业务（由 EMS/NIU 提供物资供应时 X.21 信到被配置成优先级较高。如果需要，这些 32 kbps 的信道可以用于高达 9600 b/s 的语音频带数据。当信道速率由于检测到传真/调制解调器开始音而变成 64 kbps PCM 编码语音/数据速率时，有可能使用至少 33.6 kbps 的传真和调制解调器速率。

这一 SU-RBU 空中链路为每一个方向的信道提供一个单独的 2.72 MHz（包括保护频带共有 3.5 MHz）信道，其间用 91 MHz 或者 119 MHz 频带隔开。标称工作频带是 2.1~2.3 GHz 或者 2.5~2.7 GHz。然而，只要发射和接收频率之间的谱屏蔽和距离符合 ITU 283.5 规范，该系统的频率就能从 1.8 变成 5 GHz。对于 ITU 283.5 规范，总共有 96 个频率对，如图 2 所示。例如，RBU 12 可以在频带 3'里发射信号，在频带 3 里接收信号，SU 14 在频带 3 发射信号，在频带 3'里接收信号。

RBU 12 可以用 2.72 MHz 的频带同时支持 128 个 34 kbps 的信道，使得它的谱效率达到 1.6 b/Hz。在这一总容量中，FWS 10 使用了 8 个信道，每一个信道的另外 2 kbps 是系统开销。这样，有效的业务承载容量是 120 个 32 kpbs 的信道。

FWS 10 的谱效率是普通 CDMA 系统的 3 到 5 倍，主要是因为 FWS 10 采用了双向同步 CDMA。可以相比的系统，包括基于 IS-95 的那些，

是异步的，或者只在一个方向上是同步的。双向同步使得 FWS 10 能够使用接近正交的扩频码并获得最大的数据容量。

在空中长距离传输的过程中无线电信号会损耗能量。为了保证远距离用户的信号不被近距离用户的信号所湮没，RBU 12 控制 SU 14 的功率。在优选实施方案里，RBU 12 只控制反向信道（从 SU 14 到 RBU 12）的功率。功率的控制主要是在 SU 14 的初始化过程中建立的。

以后，很少进行功率调整，功率调整要根据瞬态环境条件进行。这一闭环功率控制是通过跟所需功率电平比较，功率不够的时候提高功率直到得到所需电平，来进行的。

由于每一个 SU 14 都只接收一个电平的信号，因此正向信道功率控制是不需要的。RBU 12 只需要保证最远处 SU 14 收到的信号的强度足够就行。

扩大范围并不总是必需的。在人口稠密的市区甚至在郊区里，需要用蜂窝方式部署系统，如下文所示。在这种情况下，为了减小扇区和小区之间的干扰，要控制 RBU 的范围和方向。可以在 RBU 12 里使用定向主天线 12b，以及控制总的 RBU 功率，来控制这一范围。

当一个 SU 14 检测到摘机信号（用户拿起电话）时，它就用划分了时隙的 ALOHA 方式在 6 个反向同步边信道中的一个上发射一个呼出请求。这一边信道是随机地选出来的。RBU 12 处理这一请求，提供一个可用的活动信道，并发送一个包括这一活动信道码（正向的和反向的）的呼出应答给 SU 14。与此同时，RBU 12 开始在这一新激活的信道里发射正向边信道数据，并在给定时间开始发射活动呼叫数据。正在收听正向边信道的 SU 14 收到这一活动信道分配指令，并在超帧边界切换成活动码。然后 SU 14 开始接收这些边信道数据和活动呼叫数据。

当 NIU 13 收到给本地环内 SU 14 的呼入时，RBU 14 通过 E1 链路获得通知。RBU 12 首先检查 SU 14 是否正占线。如果不占线，RBU 14 就在正向边信道上发送一则消息给 SU 14，这一消息包括活动信道码。然后呼叫处理按照上述呼出处理相同的方式进行下去。

如果所有信道都占线，而且 NIU 13 收到给没有占线的 SU 14 的一个呼入，它就给主叫方发去一个用户忙的信号音，除非被叫 SU 有入站接入的优先权（例如医院、消防队或者警察），在这种情况下，NIU

13 让 RBU 12 断开优先级最低的呼叫，为被叫 SU 14 准备好一个信道。类似地，如果 SU 14 发出一个业务请求而没有空闲信道，那么 RBU 12 就在一个临时业务信道上给出拨号音，并接收所拨号码。如果所拨号码是一个紧急号码，RBU 12 就断开优先级最低的呼叫，空出一个业务信道，跟 SU 14 连接起来。如果被接号码不是紧急号码，SU 14 就给出一个特殊的忙音，说明“等待服务”状态。

现在参考图 3 更详细地介绍 RBU 12 和 SU 14.

来自 PSTN 13a 的呼入经过 NIU 每信道 13~64 kbps 的 E1 干线 13b，然后到达 RBU 内的 E1 接口 20。这一 E1 接口 20 有选择地完成 A 律 ADPCM 算法，将 64 kbps 信道压缩成 32 kbps 信道信号，放入 PPCM 干路 21 的时隙。如果绕过了 A 律 ADPCM 压缩，这一 64 kbps 信道就被分成两个 32 kbps 信道，并放入 PPCM 干路 21。在这一优选实施方案里，RBU 12 可以支持多达 128 个 32 kbps 的信道，每一个 SU 14 都可以支持多达 4 个 32 kbps 的信道。这一 PPCM 干路 21 利用帧同步（FrameSync）信号 20a 进行工作，该信号是每 16 ms 产生一次的定时脉冲。来自和去往 RBU 12 的所有呼叫都经过 PPCM 干路 21 和 E1 接口 20。如果是呼入，就将信号传递给一个基带合并器（BBC）22，经过一个 D/A 变换器 24 和一个射频前端（RFFE）26，再传递给天线 12b，发射给 SU 14。在 SU 14 里，天线 14a 收到呼入信号，传递给接收 RFFE 34、A/D 36、解调器 38 和接收机 40。SU 14 包括一个用户线接口电路（SLIC）42，它将一个脉码调制（PCM）干路 43 跟网络终端单元（NTU）52 连接起来。在相反方向上，NTU 52 发出呼叫，经过 SLIC 42 和 PCM 干路 43 到达发射机 44、调制器 46、D/A 变换器 48 和发射 RFFE 50。这一信号到达 SU 天线 14a，并被 RBU 天线 12b 收到。收到的信号传递给接收 RFFE 28、A/D 变换器 30、解调器和同步单元 32，然后经过 PPCM 干路 21 和 E1 接口 20，通过 E1 干路 13b 跟 PSTN 13a 和 NIU 13 连接。

RBU 12 为整个 FWS 10 控制主时序。整个 FWS 10 的时序都以 PPCM 干路 21 产生的周期性定时脉冲为基准，也就是以 FrameSync 信号 20a 为基准。在 FWS 10 里，所有数据都分组构成等尺寸叫做帧的数据包，然后将这些帧组成超帧，例如，用三帧组成一个超帧。

下面参考图 5A 和 5B 说明当前最好的 S-CDMA 波形发生电路。在

RBU 12 里，数据（32 kbps）和控制消息（1.5 kbps）被多路复用器（MUX）53 复合成一个比特流（34 kbps）. 在方框 54 里，对这一数据流进行 1/2 速率卷积编码，然后在方框 56 里收缩成 4/5 速率（4/5 速率收缩栅格码），产生 I 和 Q 码元对. 然后 SYNC 插入 MUX 58 将未编码 SYNC 字（312.5 码元/秒，I SYNC 和 Q SYNC）插入每一帧的开头. 得到的 I/Q 码元对（21.25 千码元/秒）分别在扩频器 60A 和 60B 里扩频，在本发明中，I 和 Q 都使用相同的 pn 码. 然后将得到的码片波形（2.72 兆码片/秒）交给 D/A 变换器 24 和发射 RFFE 26，在那里将波形上变频到发射频率。

正向（下行）和反向（上行）信道的波形都相同，但只有正向链路每三个同步字翻转一次. 翻转过的同步字使得 SU 14 能够找到超帧的边界. 在反向链路上的同步字不翻转，因为 RBU 12 已经知道超帧的边界. 但是，反向信道是用超帧同步的，这样，边信道就可以用划分了时隙的 ALOHA 多址协议工作了. 反向信道这边信道的脉冲串总是开始和终止于超帧边界。

图 5B 的 RF 接收机将收到的信号下变频到基带. 在解扩器 62A 和 62B 里又一次用同样的 pn 码将基带信号解扩，并在累加器 64A 和 64B 里累加一个码元周期，得到 I 和 Q 软码元判决. 将 I/Q 软判决结果提供给 SYNC 检测和去除电路块 66. 块 66 的电路产生一个帧同步信号，由去收缩（depuncture）块 68 和维特比译码器 70 用于帧同步. 将 I/Q 软判决提供给去收缩块 68，在那里，收缩数据被重新插入. 去收缩块 68 的 I/Q 输出是维特比译码器 70 的输入，维特比译码器 70 接收 I/Q 码元并输出收到的数据和控制信号. 块 72 利用帧同步信号产生一个控制帧同步信号. 该信号被去复用器（DEMUX）74 用于分离数据和控制消息。

通过在 I 和 Q 信道里使用同样的 pn 码，跟采用不同的 I 和 Q pn 码的系统相比，FWS 10 的容量提高了一倍.

参考图 4，数据和控制消息包含在 16 ms 的帧 80 里. 每 16 ms 的帧 80 包括 4 个 16 字节的块或者数据字段 80A 和 3 个 1 字节的控制（CTRL）块或者字段 80B. 一个控制消息帧 82 有多个 1 字节字段，具体而言就是可以用于识别控制消息类型的一个控制消息报头字段、两个控制数据字段和两个 CRC（XOR 加密）数据完整性字段. 字段

数可以不同。控制消息帧 82 需要发射一个以上的数据帧 80。每一个数据帧 80 都开始于 1 字节的同步（SYNC）字 80B。这一 SYNC 字 80C 是没有编码的。相反，它是在收缩以后以码元速率插入 SYNC 插入 MUX 58 的，在去收缩和译码以前从 SYNC 检测和去除块 66 里去掉。SYNC 字 80C 由 RBU 接收机用来获得帧同步。SYNC 字 80C 还被维特比译码器 70 用来去掉上变频和下变频带来的 I/Q 相位模糊性。

如上所述，在传统的方法里，控制消息被放进一个队列里以便尽早发射出去，帧结构一般都被设计成在帧的开头或者结尾在一个块里发射某一帧的所有控制信息。但是，在帧头或帧尾在一个单独的块里发射某一帧的所有控制信息会导致延迟，从而使接收机的消息和电话数据出现延迟。

根据图 4 所示的帧结构，控制消息不必延迟整整一帧。而是可以在 3 个 1 字节控制块的第一个里发射，它们散布在帧数据字段 80A 里，从而显著地缩短了延迟。这还能够缩短电话数据的延迟。也就是说，通过在数据帧 80 里用“数据包”发送控制消息，电话数据的延迟更短。这一功能使得 FWS 10 能够实现更紧的控制环并减少建立和断开信道所需要的时间。

虽然介绍本发明时涉及到了优选实施方案，但对于本领域里的技术人员而言，显然可以在形式和内容上对这些实施方案进行修改而不会偏离本发明的范围和实质。

说 明 书 附 图

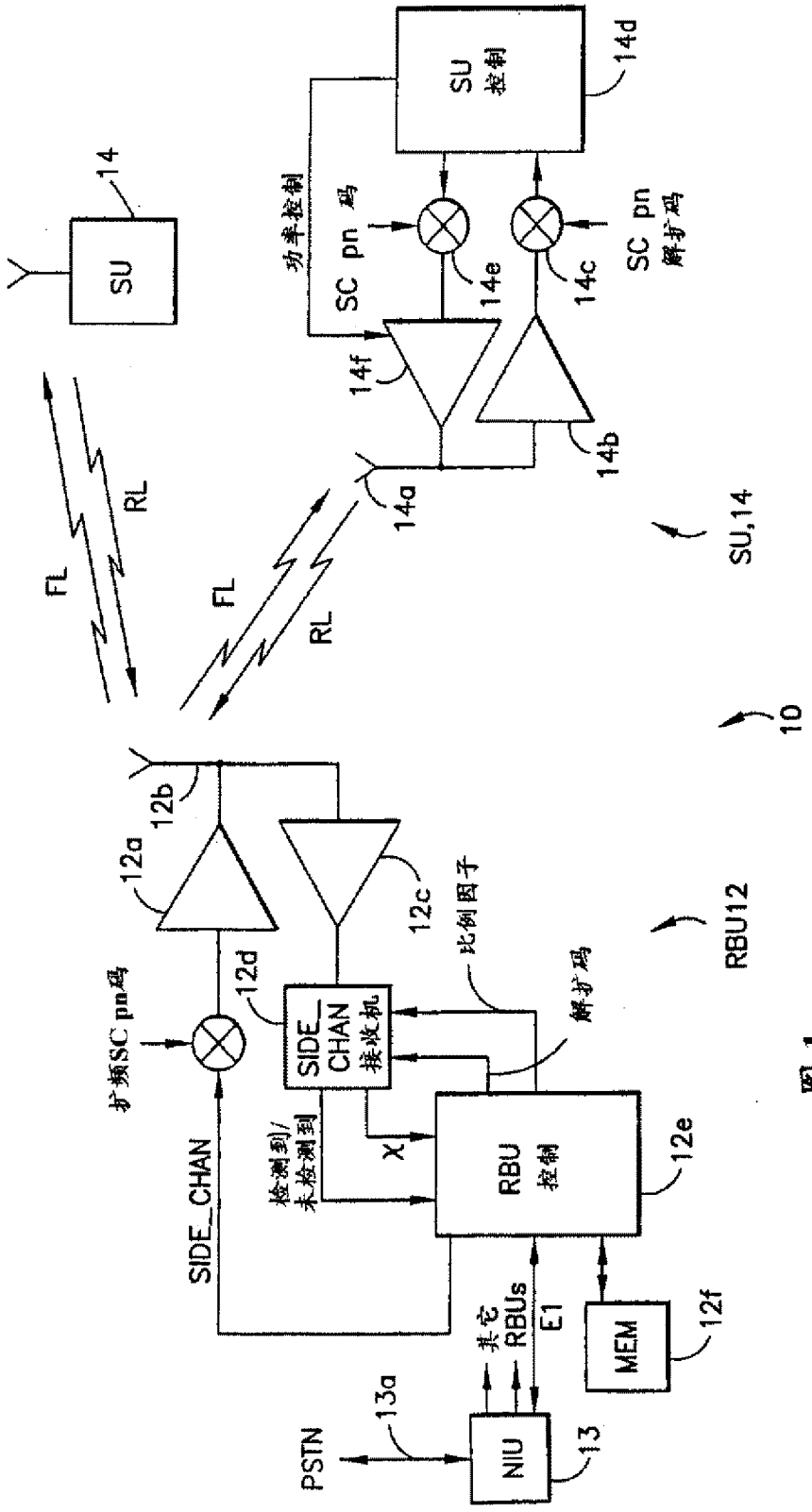

SU
14
SU,14
SU 控制
14d
功率控制
SC pn 码
14e
14c
SC pn 解扩码
14f
14b
14a
FL
RL
FL
RL
10
12b
12a
12c
比例因子
RBU12
扩频SC pn码
12d
SIDE_CHAN 接收机
解扩码
检测到/未检测到
X
RBU 控制
12e
SIDE_CHAN
其它 RBUs
E1
MEM
12f
PSTN
13a
NIU
13

图 1

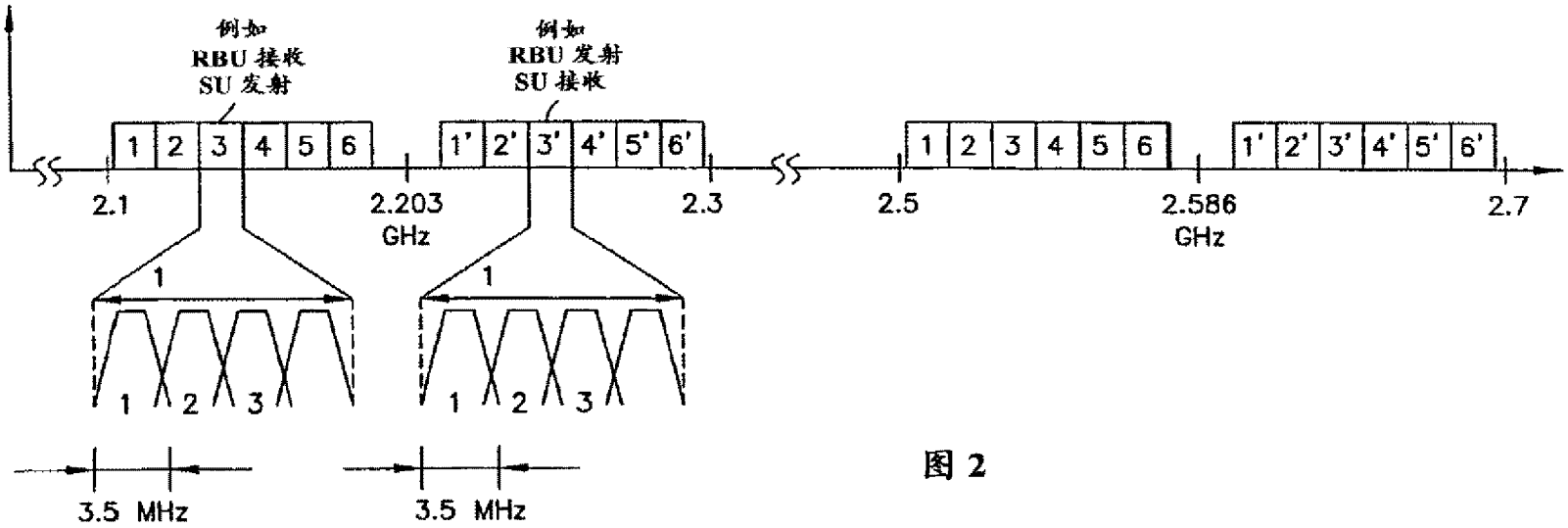

例如
RBU 接收
SU 发射
例如
RBU 发射
SU 接收
1
2
3
4
5
6
1'
2'
3'
4'
5'
6'
2.1
2.203
GHz
2.3
2.5
2.586
GHz
2.7
1
1
2
3
1
2
3
3.5 MHz
3.5 MHz

图 2

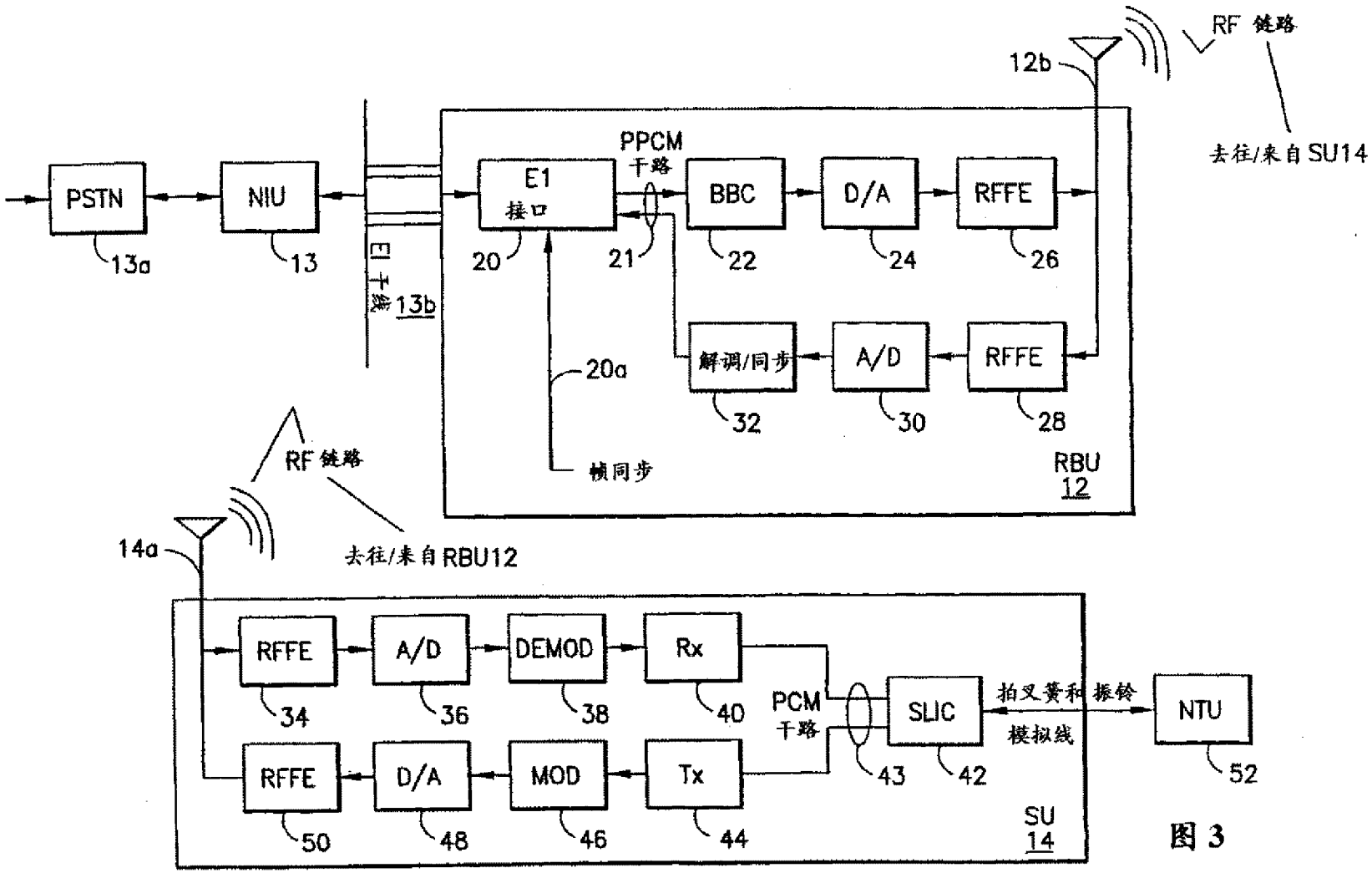

RF 链路
12b
去往/来自SU14
PSTN
NIU
13a
13
E1干线
13b
E1
接口
20
PPCM
干路
21
BBC
22
D/A
24
RFFE
26
20a
帧同步
解调/同步
32
A/D
30
RFFE
28
RBU
12
RF 链路
14a
去往/来自RBU12
RFFE
34
A/D
36
DEMOD
38
Rx
40
PCM
干路
SLIC
43
42
拍叉簧和振铃
模拟线
NTU
52
RFFE
50
D/A
48
MOD
46
Tx
44
SU
14

图 3

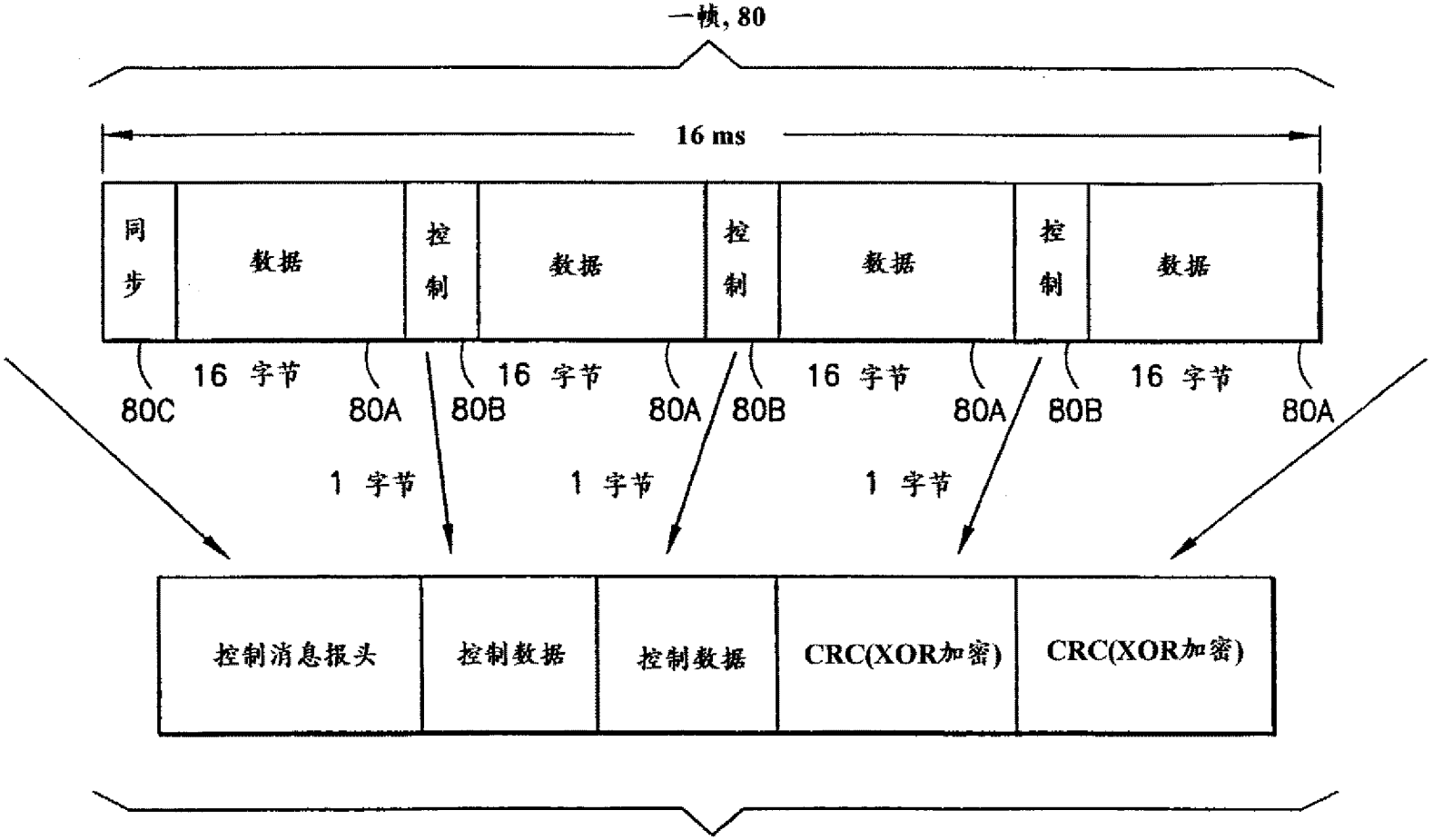

一帧, 80
16 ms
同步
数据
控制
数据
控制
数据
控制
数据
16 字节
16 字节
16 字节
16 字节
80C
80A
80B
80A
80B
80A
80B
80A
1 字节
1 字节
1 字节
控制消息报头
控制数据
控制数据
CRC(XOR加密)
CRC(XOR加密)
控制消息帧, 82

图 4

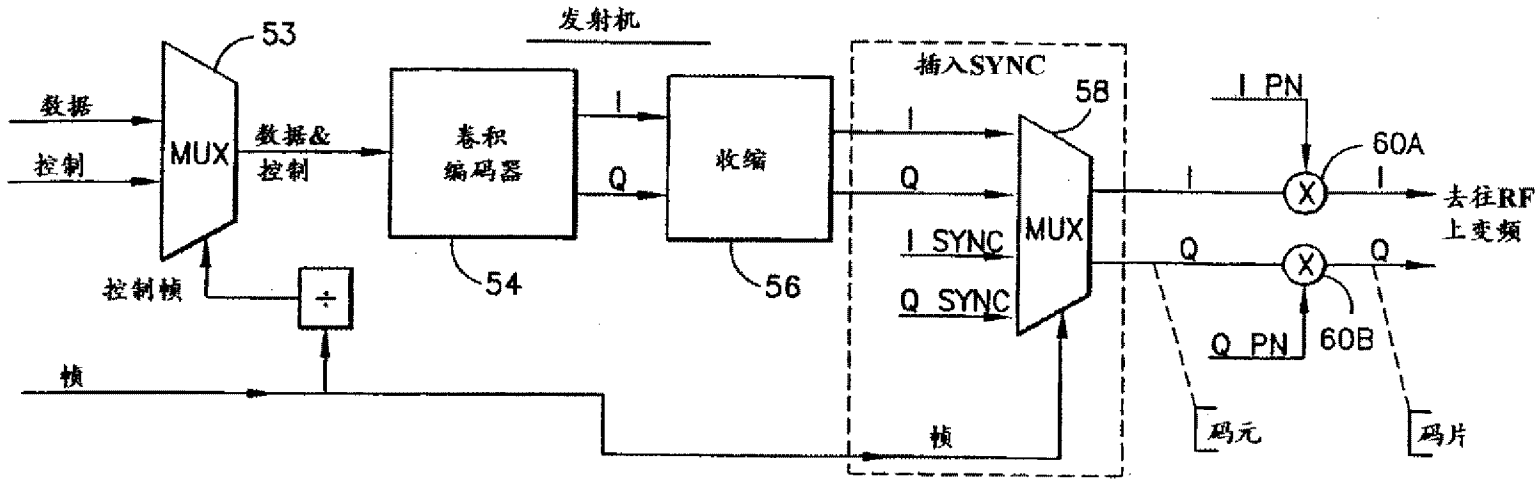

发射机
53
数据
控制
MUX
数据&
控制
卷积
编码器
54
I
Q
收缩
56
插入SYNC
58
I SYNC
Q SYNC
MUX
I PN
60A
Q PN
60B
去往RF
上变频
控制帧
÷
帧
码元
码片

图 5A

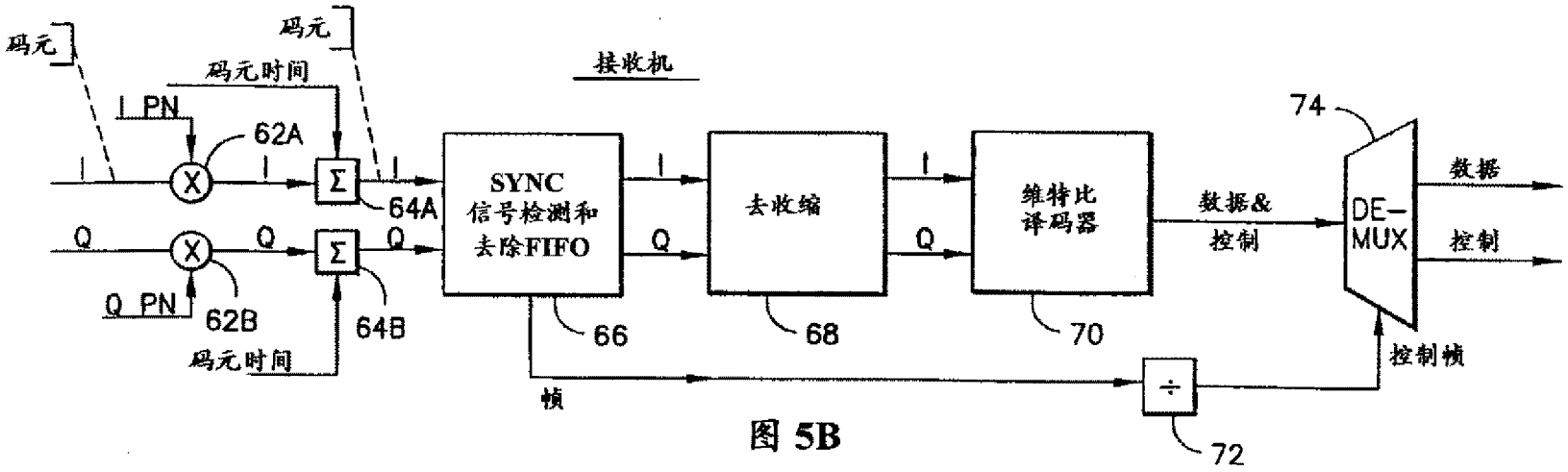

码元
码元时间
I PN
62A
Q PN
62B
码元时间
64A
64B
接收机
SYNC
信号检测和
去除FIFO
66
去收缩
68
维特比
译码器
70
数据&
控制
74
DE-
MUX
数据
控制
控制帧
帧
÷
72

图 5B

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 024 661 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
02.08.2000 Bulletin 2000/31

(51) Int. Cl.[7]: **H04N 5/445**

(21) Application number: **00101533.8**

(22) Date of filing: **26.01.2000**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **27.01.1999 US 238127**

(71) Applicant:
Hughes Electronics Corporation
El Segundo, California 90245-0956 (US)

(72) Inventors:
- **Gagnon, Gregory J.**
  Torrance, California 90277 (US)
- **Toellner, Jon D.**
  El Segundo, California 90245 (US)

(74) Representative:
Grünecker, Kinkeldey,
Stockmair & Schwanhäusser
Anwaltssozietät
Maximilianstrasse 58
80538 München (DE)

(54) Pictographic electronic program guide

(57) A system and method for displaying a pictographic program guide (PPG) to assist users in determining and selecting television viewing options and related services is described. The PPG is constructed at receiver stations based on data periodically received via a Direct-to-Home (DTH) satellite communication system. Preferably, the data decoder of the receiver station is a personal computer or a device having similar processing power. The PPG includes still pictures, live video broadcasts, still graphics, moving graphics, web pages, links and "buttons" that are utilized by the viewer to perform a variety of operations, including determining program availability, selecting programming or services, and launching to related information, programming or services. The PPG layout and organization is defined by one or more templates, and the basic instructions for building the templates are broadcast to the receiver stations. The PPG, according to the present invention, is constructed from both real time broadcast data ("streaming" data) and periodically downloaded and stored data ("file" data). By broadcasting the template information, along with instructions or linking-data on how to fill in the template using the streaming and file data, the broadcaster can easily change the PPG presentation format by changing the broadcast template information.

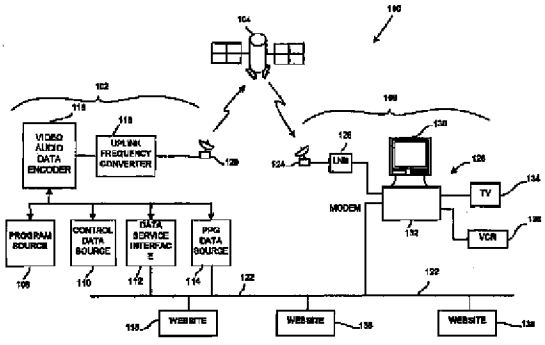


FIG. 1

EP 1 024 661 A2

Description

BACKGROUND OF THE INVENTION

(a) Field of the Invention

[0001] The present invention relates in general to entertainment broadcast systems that transmit and receive a wide variety of video, audio, software and other types of data. More particularly, it relates to a multi-channel broadcast system that transmits a video/text/graphic-based program guide data stream that is used at viewer stations to generate a user interface that facilitates a user's selection of various programs and services.

(b) Description of Related Art

[0002] The use of electronic communications media to provide access to large amounts of video, audio, textual and data information is becoming more frequent. For example, the public switched telephone network (PSTN) is routinely used to transmit low speed digital data to and from personal computers. Cable television infrastructure is used to carry, via coaxial cable, analog or digital cable television signals, and may also be used to provide high speed Internet connections. In general, cable television infrastructures include many head end or transmission stations that receive programming from a variety of sources, then distribute the programming to local subscribers via a coaxial cable network. Large Direct-to-Home (DTH) satellite communications systems transmit directly to viewers over one hundred fifty audio and video channels, along with very high speed data. DTH systems typically include a transmission station that transmits audio, video and data to subscriber stations, via satellite.

[0003] One particularly advantageous DTH satellite system is the digital satellite television distribution system utilized by the DIRECTV® broadcast service. This system transports digital data, digital video and digital audio to a viewer's home via high-powered Ku-band satellites. The various program providers send programming material to transmission stations. If the programming is received in analog form, it is converted to digital. The transmission stations compress the digital video/audio programming (if needed), encrypt the video and/or audio, and format the information into data "packets" that are multiplexed with other data (e.g., electronic program guide data) into a plurality of bitstreams, which include identifying headers. Each packetized bitstream is modulated on a carrier and transmitted to a satellite, where it is relayed back to earth and received and decoded by the viewer's receiver station. The receiver station includes a satellite antenna and an integrated receiver/decoder (IRD). The IRD may be connected to appropriate output devices, typically including a video display.

[0004] In general, DTH satellite(s) broadcast on several frequencies from multiple transponders at differing polarizations (e.g., left and right hand circular polarization), and each transponder bitstream includes the video and audio data packets (in a compressed format) for several different programs (or "viewer channels"). For example, transponder one may broadcast the digital video and audio data packets for ESPN, TNT, AMC, A&E, E!, STARZ and USA, in a statistically multiplexed fashion. Satellites or other distribution systems which require separate input processing (e.g., satellites at two separated locations requiring different antennas) may also be used. Accordingly, in order to receive a desired viewer channel, the receiver station must know the transponder frequency and the polarization at which the desired signal information is being broadcast by the satellite, along with the identifying header information for those data packets on that transponder that relate to the desired program to permit its isolation from the multiplexed bitstream.

[0005] Each satellite transponder broadcasts a program guide data stream, which typically includes not only broadcast schedule data, but also the aforementioned information that the receiver station needs in order to tune to a particular channel. The program guide data stream is broadcast on all satellite transponders so that channel selection information is always available to the IRD regardless of the channel to which the IRD is tuned.

[0006] The data packets are distinguished from one another by their header information, which is referred to as the packet's "service channel ID" (SCID). For example, if a viewer instructs the IRD to display ESPN, the IRD, via the tuning information in the program guide data stream, determines the transponder frequency and polarization at which the ESPN programming is broadcast, along with the SCIDs of the data packets that are needed to generate and display the video, audio, and data content of the ESPN program.

[0007] The scheduling data in the program guide data packets also provide channel and program-attribute information that is used by the IRD to construct and output as a viewable display (which may be a full or a partial screen) a text-based listing of programming channels, times, titles, descriptions, ratings, etc. In operation, a program guide display is typically presented as a grid having channels listed along the left, times across the top, and program titles shown within the grid squares. Users can scroll through the grid, either up and down (by channel) or to the left and right (by time). Channels can be selected by inputting the channel number directly using the number keys on a user's remote control, or channels may be selected from the program guide display by highlighting and selecting a currently broadcast program that is listed in the grid. In either case, the IRD tunes to the chosen channel by accessing the channel's transponder (frequency), polarization, and SCID information denoted by the program

guide data stream.

[0008] An extension of known IRD equipment is a PC-based system that allows users to receive, directly into their PC's, the same digital video, audio, and related information signals received in conventional DTH systems. The receiver station in this PC-based system includes a local satellite receiver dish similar to that of a conventional IRD system, but the IRD functions are implemented within the PC architecture through the use of one or more circuit boards that are inserted into the PC. The decoded outputs from these boards are displayed on the PC's monitor, or may be output to a conventional video display (e.g., a television set) and/or other mass storage medium such as magnetic tape, digital video disk (DVD), optical or magnetic disk, video recorder (VCR), etc. Because the receiver station includes a personal computer, a large number of additional data and software-related services can also be downloaded directly to the PC, thereby offering a variety of services, including broadcast programming, pay-per-view events, audio programming, data services, web-casting, software downloads and other data or software-related services.

[0009] One example of a known electronic program guide is described in U.S. Patent No. 5,633,683, entitled "Arrangement And Method For Transmitting And Receiving Mosaic Video Signals Including Sub-Pictures For Easy Selection Of A Program To Be Viewed", issued May 27, 1997 to Rosengren et al. The Rosengren et al. patent discloses a video-based electronic program guide, wherein the available programs are conveyed to the viewer by displaying a so-called "mosaic" made up at the broadcast site of the live video from each of the transmitted channels. The mosaic is essentially a single image divided into a plurality of areas, wherein each area displays the live video of one of the available programs. A user selects a channel by moving a cursor over the video area displaying the desired programming, then pressing a select button on either the television or the user's remote control. The selected live video image is then tuned and displayed. In an alternative embodiment, the live video in any area of the mosaic is automatically replaced with a still picture of the program if it is determined that the live broadcast is currently a commercial instead of the actual program.

[0010] Another video-based electronic program guide is disclosed in a European patent application entitled "Television Signal Transmission And Reception System With Multi-Screen Display For Tuning Operation," published May 25, 1994 and bearing publication no. 0 598 576 A2 (filed by Toshiba). The Toshiba EPO application, like Rosengren et al., discloses a video-based electronic program guide wherein the available programs are conveyed to the viewer by displaying a so-called "multi-screen" display made up at the broadcast site of live video from each of the transmitted channels. The multi-screen is essentially a single screen divided into a plurality of areas, wherein each area displays the live video of one of the available programs. A user selects a channel by moving a cursor over the video area corresponding to the desired programming, then pressing a select button on either the television or the user's remote control. The selected live video image is then tuned and displayed in the full screen. In an alternative embodiment, the video-based program guide is applied to a two-way CATV system, and the viewer's initial request for program guide information is sent back to the broadcast center which transmits to the viewer a text listing of categories into which the available programs and channels have been divided. The viewer selects a category, and this category selection is transmitted back to the broadcast center which may then transmit another listing of subcategories related to the chosen category. The viewer continues to select subcategories until no further subcategories are available, at which time the broadcast center transmits a multi-image screen containing only the video images from those programs that fall in the selected category and subcategories.

[0011] U.S. Patent No. 5,523,796, entitled "Video Clip Program Guide" and issued to Marshall et al. on June 4, 1996, discloses a text-based program guide laid out in a grid. Video clips from certain programs are stored at the viewer's station, and the programs that have video clips available are shown in the grid program guide with an icon next to the program's title. A viewer who desires to see a video clip selects the icon associated with the program, and the viewer station runs the video clip in a portion of the screen. The rest of the screen displays text information such as the program's title, channel, start and end times, content description, etc. Other program guide and/or multi-image systems are disclosed in U.S. Patent Nos. 5,231,493; 5,422,674; 5,398,074; 5,430,486; 5,434,624; 5,442,398; 5,452,012; and 5,047,867.

[0012] While known program guides have advantages, there is still room for improvement, particularly when considering the large number of data, software, video, audio, pay-per-view and other programming services available through present and future DTH satellite broadcast services. For example, the viewable display generated from electronic program guide data tends to be presented primarily as text laid out in a grid. The processing power of currently available IRD's, while appropriate for current DTH programming services, inherently limits how the program guide can be displayed, how much information can be incorporated into the guide, and how quickly and efficiently a user can move through the guide. These program guides are therefore essentially limited to conveying program availability and tuning information, and do not have the organization and flexibility to effectively support other services such as software downloads, webpage links and downloads, data services, and other functions.

[0013] Accordingly, for broadcast systems having a large number of services that deliver a large amount of

data to relatively sophisticated receiver stations (e.g., a PC), there is a need for a broadcast electronic program guide and an associated viewable display format and content that significantly enhances how the program guide can be displayed, how much information can be incorporated into the guide, and how quickly and efficiently the user can move through the guide.

SUMMARY OF THE INVENTION

[0014] The present invention provides a method and apparatus for efficiently and effectively transmitting, receiving, organizing and selecting transmitted data. The method and apparatus of the present invention is preferably embodied in a user interface and related data protocols and procedures. The user interface may be implemented in the context of a wireless distribution system for securely, reliably and inexpensively distributing video, audio, data service, software and other services to geographically remote receiver stations. The wireless distribution system is preferably a DTH digital satellite television distribution system, though other systems (e.g., terrestrial wire, cable, or wireless broadcast) may also be used in other embodiments. A typical DTH digital broadcast system includes a transmission station, a satellite relay, and a receiver station. At the transmission station, video and audio programming signals are digitized in known manners, multiplexed with other data signals (such as the data needed to construct a program guide display according to the present invention), compressed (if required), encoded, mated with error correction codes, modulated on carriers, and uplinked to a geosynchronous satellite. The satellite receives the uplinked signals and rebroadcasts them over a footprint that preferably covers a predetermined geographical area, for example, the continental United States. Receiver stations, which are typically located at the user's home or business, receive the satellite signals. The receiver stations each include an antenna, which preferably is in the form of a satellite dish, along with an integrated receiver/decoder (IRD). The antenna feeds the received satellite signal to the IRD unit which recovers the originally transmitted digital video, audio, and data. Other receiver station equipment (e.g., cable decoder units) may be used with other distribution systems in other embodiments, as is well known in the art.

[0015] The present invention is particularly applicable to a receiver station having sufficient processing power to process and generate a program guide display and associated features that goes beyond conventional video/text/grid program guides. The processing power may be incorporated directly into the IRD, for example, by adding a more powerful microprocessor, more memory, and associated software to the conventional IRD circuitry. Alternatively, the receiver station IRD may be replaced with a PC having circuit cards that perform the IRD functions. A PC-based system significantly increases the receiver station's processing power, along with the number of services (e.g., data services and software) the receiver station can receive and use. Accordingly, the features of the present invention are most advantageously utilized by a PC-based (or comparable) receiver station.

[0016] A PC-based receiver station suitable for use with the present invention includes an antenna, which preferably is in the form of a satellite dish, along with a PC which, like the above-described IRD, recovers the originally transmitted digital video, audio, and data. The digital broadcast data received from the satellite dish is coupled directly into a transport circuit board within the PC. The PC's transport circuit board also performs initial circuit functions on the signal coupled in from the antenna, including tuning, demodulation, and forward error correction (FEC). The transport circuit board within the PC also performs similar functions to that of the IRD's transport circuit, including channel de-multiplexing, decryption and access determination. The received digital broadcast data is sent from the transport circuit to video/audio decoder circuits, which may be on the same or separate circuit board. The video/audio decoder circuit board decompresses and/or decodes the received compressed broadcast signal.

[0017] In one embodiment of the present invention, the transmission station transmits to the receiver stations program selection data/information that is used at each receiver station to construct an electronic program guide and associated display format and content (i.e., a user interface) that, in contrast to known video-based and/or text/video/icon-based electronic program guides, significantly enhances how the program guide can be displayed, how much information can be incorporated into the guide, and how quickly and efficiently a user can move through the guide. The viewable display format, according to the present invention, incorporates moving picture video, still pictures, text, links to external data sources, graphics and other features that facilitate the selection of various programs and services.

[0018] The transmission station (e.g., uplink facility) transmits to the receiver stations the pictographic program guide (PPG) data/information needed at each receiver station to construct the PPG display. The broadcast PPG data can be divided into three categories. The first is real time conventional text/grid-based program guide data. The conventional guide data includes schedule and program attribute information, along with information that the receiver station needs in order to tune to a particular channel. In a typical DTH system, the conventional program guide data stream is broadcast on all satellite transponders so that channel selection information is always available to the receiver station regardless of what channel the receiver station is tuned to. In general, tuning the receiver station to a particular channel requires knowledge of at least the satellite transponder on which the channel is broadcast, along with polarization information and information identifying which data packets on that transponder cor-

respond to the channel of interest.

[0019] The second category of broadcast PPG data may be referred to as "streaming" data, which is real time PPG data transmissions other than the conventional guide data. Streaming data can cover a variety of data types including, for example, "ticker" data (stocks, sports scores, etc.) and PPG "template" data (i.e., instructions to the receiver station on how to construct and lay out the display of the PPG).

[0020] The third category of PPG data may be referred to as PPG "file" data. PPG file data is periodically (e.g., once a day at 2:00 a.m.) downloaded to the receiver station and stored in memory. File data includes various information that is related to the PPG but is sufficiently static so that it does not need to be sent in real time. For example, the transmitted file data may be still pictures related to various channels and/or services and used to construct a portion of the PPG display, moving video clips related to the various channels and/or services and used to construct a portion of the PPG display, Web pages related to the various channels and/or services, and linking information that identifies and provides access to related information. The links may connect to either internal resources (e.g., cached Web pages) or to external resources (e.g., a URL to an external Web site). If the DTH broadcast system includes a software feature known as "webcasting," the file data may include a data catalog indicating the webcasting broadcast schedule. In general, webcasting involves accessing at the uplink a variety of web sites from the world-wide web, and broadcasting those web sites to the subscriber stations at selected times. Viewers wishing to receive a particular website would access the data catalog to determine the broadcast time and channel, and tune their receiver to that channel at the designated time.

[0021] Several examples of a particular PPG template embodying the present invention are shown in FIGS. 2-5. As shown in FIG. 2, for example, the layout/content of the illustrated PPG screen 220 includes five major segments. The first segment is an active video segment 222 that displays the video/service channel to which the receiver is currently tuned. The second segment is a category segment 226. All of the available channels are divided into categories such as sports, movies, news, data services, etc., and these available categories are listed in the category segment 226. Each category has its own template instructions that may be different from or the same as the templates in other categories. If the number of programs/services in a given category is more than fits on a single template, additional templates in the form of additional template "pages" are created for that category. Selecting a particular category selects the template page(s) that present the programming/service that fall under that category. A third segment, the "page" segment 232, allows the user to move around the various pages of a template by selecting the page segment 232.

[0022] The fourth segment is a video/picture segment 228 shown as a matrix of six 3:4 aspect ratio areas each representing a programming channel or service channel that may be accessed by the receiver station. Selecting one of the video/picture areas selects the channel associated therewith. The areas are linked to the program guide tuning information in the same way that the display text-based grids and channel numbers are linked to the tuning information. Accordingly, selecting the video/picture area that represents ESPN, links the receiver to the program guide tuning information (transponder and SCID) needed to acquire the program currently being broadcast on ESPN. An additional feature is an information area that can pop up (overlaying a portion of the current display) whenever a cursor moves over a given video/picture area. The information area could provide any desired information about the program, for example, the title, program description, program duration, program rating, etc.

[0023] The fifth segment is the "link" segment, which can be found in various areas on a given screen. The "links" include graphical interface "buttons" and other graphic symbols for selecting certain features and/or launching the PPG into various states are provided for the active video segment 222, the video/picture segment 228 and special auxiliary areas 234, located at the bottom of a given template page. Each link, like the video/picture areas, represents a related channel, service or other information that can be accessed from the PPG. Selecting a link may initiate a series of local interactions involving primarily the receiver station hardware, or the link may initiate external interactions with other hardware/systems such as the Internet. For example, "web" links allow the viewer to either "pull-up" a related web page stored at the receiver station or launch to external equipment/systems to access the web-page information, grid-guide links allow the viewer to move from the PPG to the grid-guide, "preview" links allow the user to select and run video clips of the program in its video/picture area, "software" links allow users to download related software (e.g., computer games, applications software or web originated software), "view" links make a given picture area active, "full" links put the associated video/picture area in the full screen, "record" links use the broadcast time and channel information associated with a program to control a video recorder to record the program at its broadcast time, "buy" links allow users to purchase pay-per-view programming or services via conventional impulse-pay-per-view purchase screens, and data-catalog links take the user to the webcaster broadcasting schedule for the system.

[0024] The PPG, according to the present invention, is constructed from both real time broadcast data ("stream" data) and periodically downloaded and stored data ("file" data). By broadcasting the template information, along with instructions on how to fill in the template using the streaming and file data, the broadcaster can

easily change the PPG presentation format by changing the broadcast template information. In operation, a user selects a category, and the channels that fall within the selected category are displayed according to a particular template format. The templates are a particular layout and configuration of graphics, still pictures, moving pictures and text representing the content of the channel and associated information and/or services. Selecting a portion of the PPG display selects the programming, channel, service or related data or operation represented by that portion of the display. Selecting a portion of the display can involve primarily local operations, or can launch to external devices/systems such as the Internet. Additionally, by limiting the number of video/picture segments that can be active at any time, the present invention avoids the confusion associated with known picture-based program guides that have from sixteen to twenty-five separate active video areas in a given screen of the guide. Thus, the program guide of the present invention provides an intuitive system and method for browsing and selecting television programming and a wide variety of broadcast services.

[0025] The invention itself, together with further objects and attendant advantages, will best be understood by reference to the following detailed description, taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0026]

FIG. 1 is a diagram of a direct-to-home (DTH) transmission and reception system capable of broadcasting and utilizing data streams embodying aspects of the present invention;
FIG. 2 illustrates an example of one "page" of a pictographic program guide embodying aspects of the present invention;
FIG. 3 illustrates an example of another "page" of a pictographic program guide embodying aspects of the present invention;
FIG. 4 illustrates an example of another "page" of a pictographic program guide embodying aspects of the present invention;
FIG. 5 illustrates an example of still another "page" of a pictographic program guide embodying aspects of the present invention;
FIG. 6 is a diagram of selected hardware processing components of the receiver station shown in FIG. 1;
FIG. 7 is a block diagram illustrating one possible system architecture within which aspects of the present invention may be used;
FIG. 8 is a diagram illustrating a type of transport data packet that may be transmitted via the system shown in FIG. 1;
FIG. 9 is a block diagram illustrating a preferred data flow through a protocol stack for use with the present invention;
FIG. 10 is a block diagram illustrating a preferred method of processing a data packet for use with the above-referenced protocol stack;
FIG. 11 is a representation of a BFDP header;
FIG. 12 is a representation of a UDP header;
FIG. 13 is a diagram of a version 4 IP packet header;
FIGS. 14A - 14D are block diagrams representing MPT packets;
FIGS. 15A and 15B are diagrams representing a BARP header and a BARP address record, respectively; and
FIGS. 16A - 16D are sample SDP + records for various information services that may be used with the present invention.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0027] To facilitate review and understanding of the invention and the preferred embodiments, the present disclosure has been organized in accordance with the headings and sub-headings shown below.

I. System Overview
II Pictographic Program Guide (PPG)
III. Receiver Station Generally
IV. Receiver Station Architecture
V. Data Packet
VI. Audio/Video Processing
VII. Data Processing

A. Protocol Stack/Broadcast File Download Protocol (BFDP)
B. Broadcast Address Resolution Protocol (BARP)
C. SDP+ Records
D. Webcast

VIII. Conclusion

I. System Overview

[0028] By the way of example only, the method and apparatus of the present invention is disclosed in connection with a system that broadcasts, via satellite, video programming, data services and multimedia data (e.g., webpages). It should be understood, however, that any system requiring intuitive interactive program and/or service selection may alternatively employ the techniques shown herein. Such systems might include other broadcast communications techniques not traditionally associated with video programming or the Internet. For example, paging or cellular systems delivering news or other information could benefit from certain aspects of the method and apparatus of the present invention.

[0029] Generally, however, the techniques of the present invention are best used by broadcast video and data systems having a large number of available programs, data and services, thereby benefitting from the simplification of programming organization and selection provided by the present invention. A preferred broadcasting system is the satellite-based system utilized by the DIRECTV® broadcast service. Such embodiments of the present invention employ a satellite receiving antenna to acquire real-time video broadcasts and periodic data broadcasts used to construct a program guide display. It should be understood, however, that many other delivery systems are readily applicable to alternate embodiments of the present invention. Such systems include wired or cable distribution systems, UHF/VHF radio frequency systems or other terrestrial broadcast systems (e.g., MMDS, LMDS, etc.), and fiber optic networks.

[0030] FIG. 1 illustrates a typical Direct-to-Home (DTH) PC-based satellite communication system 100 capable of utilizing the present invention. The system 100 includes a transmission station 102, a satellite/relay 104, and a plurality of receiver stations, one of which is shown at reference numeral 106. Wireless communications are provided between the transmission station 102, the satellite/relay 104, and the receiver station 106. The transmission station 102 includes programming sources 108, a control data source 110, a data service source 112, one or more program guide data sources 114, a video/audio/data encoding system 116, an uplink frequency converter 118, and an uplink antenna 120. The data service source 112 receives data service information and webpages made up of text files, graphics, audio, video, software, etc. from a network 122 (e.g., the Internet, a LAN or a WAN). The satellite/relay 104 is preferably at least one geosynchronous or geo-stationary satellite. The receiver station 106 shown in FIG. 1 includes a reception antenna 124 connected to a low-noise-block (LNB) 126, and an integrated receiver/decoder (IRD) embodied in a personal computer (PC) 128 having a monitor 130 and a computing unit 132. Other devices, such as another video display device (e.g., television) 134 and a video recorder 136 (e.g. VHS, DVHS, DVD, etc.), may also be supported, if desired.

[0031] In operation, the programming sources 108 receive video and audio programming from a number of sources, including satellites, terrestrial fiber optics, cable, or tape. The received programming signals, along with data signals from the control data source 110, the data service source 112, and the program guide data sources 114, are sent to the video/audio/data encoding system 116 where they are digitally encoded into information data streams that are multiplexed into a packetized data stream or bitstream using a number of conventional algorithms. Each data packet within the packetized data stream includes a header that identifies the contents of the data packet and a service channel identifier (SCID) that identifies the data packet. In a conventional manner, the encoded bitstream is modulated and sent through the uplink frequency convener 118, which converts the modulated encoded bitstream to a frequency band suitable for reception by the satellite/relay 104. The modulated, encoded bitstream is then routed from the uplink frequency converter 118 to the uplink antenna 120 where it is broadcast toward the satellite/relay 104. The satellite/relay 104 receives the modulated, encoded bitstream and re-broadcasts it downward toward an area on earth that includes the receiver station 106. The reception antenna 124 of the receiver station 106 receives the signal, which is typically shifted from, for example, the Ku-band signal down to, for example, an L-band signal by the LNB 126. The LNB output is then provided to the PC 128, the television 134 and/or the video recorder 136. As noted above, the PC 128 includes conventional IRD functions (provided, for example, by plug-in circuit cards (boards). Thus, when the user commands the PC 128 to tune to a particular program, the PC 128 associates the user's program selection with a transponder and SCID number and tunes the IRD to receive data packets from the appropriate transponder and to select data packets having the appropriate SCID number from the multi-program data stream.

[0032] Although not necessary for proper operation of the disclosed system, the receiver station 106 may optionally incorporate a connection (e.g., Ethernet circuit or modem) to the network 122 for transmitting requests and other data back to the transmission station 102 or other location (or a device managing the transmission station 102 and overall flow of data in the system 100) and for communicating with network devices 138 (e.g., websites) that may be on the network 122.

[0033] In general, the software executed by the PC 128 includes many conventional PC operations used to generate a pictographic program guide (PPG) having a mouse-controlled cursor or the like, windows, dialogue boxes, buttons, and other such features that facilitate user selection of various options. The PPG of the present invention is assembled using two basic types of external data: (1) real-time broadcast data (e.g. streaming data), and (2) file data (i.e., data that is periodically downloaded and stored). Real-time data includes conventional program guide data (e.g., program attribute data, tuning data, etc.), ticker data (e.g., stocks, sports scores, etc.), some SDP+ records, and announcements (e.g., updates to the webcast data catalog, etc.). File data includes information that is updated periodically such as still pictures, moving video clips, webpages, data catalog (webcast schedule), links to other internal or external sources of information, and various discrete software downloads. The PPG of the present invention organizes and simplifies the presentation of real-time broadcast data and file data by providing, inter alia, a plurality of pages, wherein each page has a display with

several distinct segments. For example, a given page type may simultaneously provide still pictures, moving videos, text, graphics, audio, and data within separate segments.

[0034] The PPG of the present invention requires the presence of appropriate data at the receiver station 106. One method of generating appropriate data and reliably transferring it to the receiver station 106 using a hardware configuration as shown in FIG. 1, is disclosed in detail below in section VII of this disclosure. Generally, the method set forth in section VII includes a data transfer technique, referred to herein as broadcast file download protocol (BFDP), that operates in a one-way broadcast communication link. BFDP is the subject of a co-pending commonly assigned application entitled _____, filed on _____ and bearing serial no. _____/_____. BFDP breaks large data files for transmission into numerous small data packets, which are labeled in a sequential manner at the transmission station 102 and broadcast to the receiver station 106. BFDP facilitates the assembly of the labeled data packets back into the large data file and enables identification of missing or corrupt data packets at the receiver station 106. Any missing or corrupt data packets at the receiver station 106 can be obtained and inserted into their correct locations in the large data file during subsequent transmissions of the large data file. Thus, if during the transmission of a large data file a number of its data packets are missing or corrupt, only the missing or corrupt data packets need be reacquired during a subsequent re-broadcast of the large data file, and not the entire large data file.

[0035] A method for resolving an Internet protocol (IP) address into a physical address is also described in section VII of this disclosure. This method is referred to herein as a broadcast address resolution protocol (BARP). BARP is the subject of a co-pending commonly assigned application entitled _____, filed on _____ and bearing serial no. _____/_____. BARP is necessary because all file data (for example a large file transferred using BFDP, as discussed above) transferred to the receiver station 106 are identified by IP addresses and, as previously noted, the receiver station 106 requires a transponder and SCID to tune to receive the broadcast file data. Accordingly, BARP allows the receiver station 106 to rapidly resolve an IP address for a desired program or service into a transponder and SCID.

[0036] To inform the user of when and on what IP address the large file mentioned above will be broadcast, session description protocol plus (SDP+) records are periodically broadcast by the transmission station 102. SDP + records are the subject of a co-pending commonly assigned application entitled _____, filed on _____ and bearing serial no. _____/_____. SDP + records are processed by the receiver station 106 to produce a schedule of all data service information that will be broadcast by the transmission station 102. Additionally, the SDP + records are used by the PC 128 to build PPG pages using selected information resident within the PC system (e.g., a basic page template) and selected dynamic data that is received from the satellite or an Internet connection. When the user launches the interface into another state or page, the PPG builds the destination page as instructed by the SDP + records and displays it on the user's PC system monitor 130. More details about the SDP + records are provided in Section I of this disclosure in connection with the descriptions of FIGS. 16A-16D.

II. Pictographic Program Guide (PPG)

[0037] Several examples of a particular PPG template embodying aspects of the present invention are shown in FIGS. 2-5. As shown in FIG. 2, for example, the layout/content of the illustrated PPG page 220 includes five major segments. The first segment is an active video segment 222 that displays the video/service channel to which the receiver is currently tuned. As shown in FIG. 2, a plurality of graphic buttons or links 224 may be displayed adjacent to the active video image 222. These graphic buttons or links 224, when selected by the user, launch the PPG into one of a plurality of corresponding states that provide additional services or data associated with the active video image 222. For example, selecting a "Grid" button transitions the active video/audio area 222 to the program grid-guide. Selecting a "Full" button may zoom the active video segment 222 to occupy a substantial portion of the display. Selecting a "Web" button could replace the video/picture segment 222 with a web page related to the currently tuned channel. For example, the "web" button could bring up on an available area of the template a list of available web pages. The list of available web pages could replace the list of categories in a category area 226 that is discussed in more detail below. Also, as discussed in more detail below, selection of the "Web" button could invoke the retrieval of webpage information that is locally cached at the PC 128 or may, alternatively, invoke the PC 128 to access various websites 138 via the Internet connection 122 to download and display webpage information as needed.

[0038] The second segment of the template 220 is the category segment 226. All available channels are classified into topics and displayed in the category segment 226 as a list of categories that includes, but is not limited to, sports, movies, family, travel, favorites, news, data services, category related web pages, etc. Topic classifications could be directed by the broadcaster, by the user, or a combination thereof. For example, a user may create a 'Favorites' category and fill it by dragging a video area from a video/picture segment 228 to the category list 226. In other embodiments, a favorites category is automatically constructed via software resident in the PC 128 that observes the user's viewing habits.

[0039] The user selects a category by positioning a cursor using a selection device such as a mouse, keys, or remote control to highlight the desired category for display. The currently selected category is displayed in an area 230 of the page 220. Each category has its own template instructions that may be different from or the same as the templates in other categories. Thus, the layout, graphics, and other content of the various templates can be optimized for the subject matter of each category. For example, the template for the "News" category could include a late breaking news banner in a portion of the display, whereas the template for the "Shopping" category could include a promotional banner advertising/featuring various products and services.

[0040] If the number of programs/services in a given category is more than fits on a single page additional pages are created for that category. Selecting a particular category selects the template page(s) that present the programming/service that fall under that category. A third segment, the "page" segment 232, allows the user to sequence through the various pages associated with a selected category template. The user may, for example, select a right facing arrow to advance through the associated pages and a left facing arrow to return to previous pages. A second page associated with the page shown in FIG. 1 is illustrated, for example, in FIG. 3.

[0041] The fourth segment is the video/picture segment 228 that preferably includes a matrix of six 3:4 aspect ratio areas each representing a programming channel or service channel, associated with the currently selected category, that may be accessed by the receiver station 106. Each video area could include still pictures, still graphics, moving graphics, live broadcasts, text, or a combination thereof representing the content of the program currently being broadcast on that channel, or for some program that will be broadcast on that channel in the future.

[0042] Delivery of the video/picture area may be accomplished via the live video broadcast, such as by freezing a frame or displaying live action or periodically sampled video. However, in preferred embodiments, the pictogram representing the program is selected by the program provider, broadcaster, or others to be a preferred, symbol, graphic, picture or other pictogram illustrative of the program content. In these embodiments, the pictogram data may be broadcast independently of the program content (e.g., well in advance for guides showing upcoming programs) via broadcast data, retrieved data, or a combination thereof. One or more of the video areas can be made "active" (i.e., the live broadcast) according to user's desires and the decoding capabilities of the user's video/audio decoder hardware/software. Accordingly, the user can have as many active video areas as desired.

[0043] Selecting one of the video/picture areas selects the channel associated therewith and displays it in the active video segment 222. The video/picture areas are linked to the conventional program guide tuning information in the same way that known text-based program grids and channel numbers are linked to the tuning information. Accordingly, selecting the video/picture area that represents ESPN, for example, links the receiver 106 to the conventional program guide tuning information (channel frequency, polarization, header ID, etc.) needed to acquire the program currently being broadcast on ESPN.

[0044] An additional feature of the video/picture segment 228 is an information area that can pop up (i.e., a child window) whenever a cursor rolls over a given portion of a video/picture area. The information area may provide any desired information about the program, for example, the title, program description, program duration, program rating, etc. Such information is typically broadcast in conjunction with known guide systems to provide users with information regarding a program.

[0045] The fifth segment is a "link" segment, which can be found in various areas on a given screen. Links (including graphical interface "buttons" for selecting certain features and/or operations) may be provided for the active video segment 222 and/or special auxiliary areas 234 located at the bottom of a given template page. In one embodiment of the present invention, links may be provided in association with (e.g., within or adjacent to) one or more of the video/picture segments 228.

[0046] When the user selects a link an action is taken. For example, "web" links may be provided that allow the viewer to "pull-up" a related webpage previously downloaded from the satellite 104 and cached in the PC 128, or that is retrieved via the network connection 122 when requested. Alternatively, selecting the "web" link could bring up on an available area of the template 220 a list of available web pages. When "grid-guide" links are selected, a conventional grid-based program guide is displayed to the user. When "preview" links are selected, the user may select and run previously stored or retrieved video clips of the program in its video/picture area. When "software" links are selected, the user may download related software (e.g., computer games, applications software or web originated software). For example, a "computer disk" button/link could be used for accessing the data catalogue of webcaster broadcasts, downloading software the next time it is broadcast, retrieving or purchasing software already cached, or for retrieving software over the network connection 122. "View" links could make a given picture area active, "full" links may expand the associated video/picture area to occupy a substantial portion of the full screen, "record" links may use the broadcast time and channel information associated with a program to control a video recorder to record the program at its broadcast time, "buy" links may allow users to purchase pay-per-view programming or services via conventional impulse-pay-per-view purchase screens, for example, a "dollar sign" button/link could be used to launch an

impulse pay-per-view process for pay-per-view programs. "Data-catalog" links could take the user to the webcaster broadcasting schedule for the system. A "lock" link could be used for controlling access to programs, for example by limiting movies to no higher than a PG-13 rating (ratings information is obtained from the grid-guide datastream). A "star" link could be selected to bring up a list of the cast in the current show. A "video tape" link could be used to launch automatic VCR programming by accessing the channel and time information from the grid-guide datastream and using that information to control the recording features of the VCR 136. A "checkbox" button/link could be used to add to a list of favorites stations or to configure a viewing agenda. A "question mark" button/link could be used for displaying additional information associated with the program, such as times, ratings, and a textual synopsis. Thus, the various links may be selected and activated by the user to launch the PPG between various states or pages. Of course, there are many other links and associated actions that could be provided.

[0047] In accordance with the present invention, a time line 236 may be provided adjacent to one or more of the active video areas 228. The time line 236 may indicate the progress of the currently running program. For example, the ends of the time line 236 may represent the respective start and finish times of the currently running program and a shaded portion of the time line 236 may correspond to the time elapsed from the start time to the current time. Thus, a user may quickly determine how much of a currently running program is available for viewing before making a viewing selection/purchase. In some embodiments, the user may be prevented from buying a pay-per-view program, for example, if less than 50% of the program remains to be broadcast.

[0048] In other embodiments, the time line 236 may be used to select a viewing time for a video/picture area. In these embodiments, scrolling back and forth in time is accomplished with arrow links, and jumping to a particular time can be performed, for example, via a calendar (not shown) that pops up when a calendar link is selected. Of course, any time selection metaphor could be used. The current time is the default, however, going forward in time allows for agenda planning, VCR programming, etc. The video picture in the video area automatically changes to the pictures appropriate for the requested guide time-frame.

[0049] The current date and time are displayed in a date/time segment 238. Moving the display time for all of the video/picture areas at once could be accomplished via a calendar or time bar or menu that could be accessed by, for example, double-clicking a mouse control on the date/time segment 238.

[0050] FIG. 4 illustrates, by way of example only, the "data" category template of one embodiment of the present invention. The video/picture segment 228 display various data delivery services. For example, a NASDAQ service channel displays a stock ticker with recent stock symbols and prices, and a sports ticker shows scores for games currently being played. The data delivered by these services is updated periodically and scrolls across the various video/picture areas 238. Persons of ordinary skill in the art will appreciate that text, graphics, video, sound, and software can be combined in various combinations to deliver content associated with data delivery services. For example, breaking CNN news headlines with video/audio clips could be transmitted as file data and stored in a designated memory location of the PC 128. Viewer's are notified of the general nature of the story and the availability of the news clip by a scroll across the live video feed for CNN, or by a pop-up "breaking news" link/button, or some other method. The viewer can access the video clip by clicking the button/link. Similarly, software (e.g., a game or new version of a spreadsheet application) could be requested and downloaded.

[0051] At the bottom of each template 220 shown in FIGS. 2-4 are auxiliary areas 234. These areas can be used in a variety of ways, such as for additional templates/buttons, advertisements, special messages, and other communications. These areas can also be used to allow various PPG services and/or operations to be launched without having to alter the basic template presentation. For example, if an impulse pay-per-view operation is initiated, the purchase screens from the grid-guide datastream could be displayed in the auxiliary areas 234 instead of the video area for that channel or the full screen, thereby allowing the purchase to proceed while still viewing the basic PPG template. Or, if a software game associated with the channel is downloaded, it can be launched and run in the auxiliary areas without having to exit the current PPG template.

[0052] FIG. 5 shows one example of a box occupying the video/picture segment 220 where enlarged live video or a web page are displayed in response to the selection of the "Full" or "Web" buttons respectively. In the present embodiment the active video segment 222 can be replaced with a logo associated with the current channel or web page, and the category segment 226 lists web pages associated with the current category. A "category" button/link under the active video/audio segment 222 allows the user to return the category segment 226 to a list of categories, thereby allowing the user to return the screen to a particular category template.

III. Receiver Station Generally

[0053] As noted above, the PPG of the present invention is preferably implemented within a DTH PC-based satellite communication system 100 such as that depicted generally in FIG. 1. Discussed in more detail below is a preferred system and method for executing the PPG software of the present invention. In particular, a preferred receiver station 106 architecture is dis-

closed. In addition, preferred data transmission methods that facilitate the PPG's ability to receive and manage the large amount and variety of digital information that is broadcast within the DTH system 100 are disclosed.

[0054] FIG. 6 is a detailed illustration of a preferred implementation of the receiver station 106 shown in FIG. 1. As shown, the receiver station 106 includes the reception antenna 124, the LNB 126, and the PC 128. The PC 128 includes the monitor 130 and the computing unit 132, which may have a modem connection via the PSTN to the network 122. The computing unit 132 includes, inter alia, a satellite receiver card 418, a video/audio decoder card 420, which may be integrated with the receiver card 418, a conditional access card 422, a mass memory such as a hard disk (not shown), and processing/control capabilities such as a PC motherboard 424. The satellite receiver card 418 includes a tuner 426, a demodulator 428, a forward error correction (FEC) decoder 430, and a transport functional processing block 432. The video/audio decoder card 420 includes a video/audio decoder 434, an optional NTSC and/or ATSC output driver 438, and a VGA output driver 436. The satellite receiver card 418 and video/audio circuits (e.g., video/audio decoder card 420) perform the functions of receiving and decoding the signal received from the LNB 126. The incoming signal is received by a satellite receiver card 418 and passed through a series of initial processing operations including the tuner 426, the demodulator 428, and the forward error correction decoder 430, before passing to the actual transport functional processing block 432. Although the functional circuits within the transport functional processing block 432 are not illustrated, they are identical to the channel demultiplexing, decryption, and access determination circuit blocks of a standard transport decoder. For example, the transport functional processing block 432 receives the transport stream or bitstream of digitized data packets containing video, audio, scheduling information, and other data. The digital packet information contains identifying headers as part of its overhead data. Under control of the PC's main processor/controller (typically located on the PC motherboard 424), the transport functional processing block 432 filters out received data packets that are not currently of interest. Received data packets that are of interest are routed through decryption and access control operations within the conditional access card 422. Access control may be provided by any known means. For example, access control may be achieved by requiring a data packet to have a proper authorization code in order to be passed to the video/audio decoder card 420.

[0055] The transport functional processing block 432 passes the data to the video/audio decoder 434 of the video/audio decoder card 420. The authorized data of interest are stored in system RAM (not shown) for buffering, and the video/audio decoder 434 retrieves the data from RAM as needed.

[0056] The allocation of memory and control functions may be arbitrarily divided between the PC system's function cards (e.g., the satellite receiver card 418, the video/audio decoder card 420, etc.). Thus, a substantial amount, or possibly all, of the control and memory functions for operation of the present invention may be integrated within a single card, or alternatively, may be incorporated within the PC motherboard 424. When needed, the data is routed to the video/audio decoder 434, which includes display circuitry. For video data, the video/audio decoder 434 reads in the compressed video data from its RAM, parses it, creates quantized frequency domain coefficients, then performs an inverse quantization, inverse discrete cosine transform (DCT) and motion compensation. At this point, an image has been reconstructed in the spatial domain. This image is then stored in a frame buffer in the video decoder's RAM. At a later time, the image is read out of the frame buffer and passed through the display circuitry to the VGA output driver 436 and optionally, to the NTSC and/or ATSC output driver 438. The display circuitry also generates the graphics that allow text such as the PPG electronic program grid guide data to be displayed.

IV. Receiver Station Architecture

[0057] Illustrated in FIG. 7 is a system architecture block diagram 500 depicting, by way of example only, a preferred organization of the PC's computing unit hardware and software which may implement aspects of the present invention. A tuner driver 502, a TV control block 504, a video MPEG driver 506, and a video VGA driver 508 provide the major functions of a conventional integrated receiver decoder (IRD). The tuner driver 502 receives a digital signal modulated on an RF carrier (e.g., a digital satellite downlink signal) on line 510, and performs known IRD functions to parse out and selectively control the flow of conditional access, video/audio, and MPT data streams. The tuner driver 502 passes selected video/audio data packets to the video MPEG driver 506 on line 512. The MPEG driver 506 controls the MPEG decoding hardware, synchronizes video and audio data, and manages the buffering of video and audio data to be displayed. The MPEG driver 506 passes decoded video information to the video VGA driver 508 via line 516. The VGA driver 508 processes the decoded video information 514 and provides a display signal that may be, for example, a standard RGB output on line 516. The TV control block 504 controls the size and location of the video window via an MPEG decode control signal on line 518 and a VGA window display control signal on line 520 that are passed to the video MPEG driver 506 and the video VGA driver 508 respectively.

[0058] With respect to file data, the tuner driver 502 passes file data (e.g., websites, software, etc.) as MPT data packets to a tuner NDIS driver 522. The NDIS

driver 522 strips the MPT header and passes standard IP data packets 524 using Microsoft® NDIS protocol to a standard Windows® Winsock® interface 526. File data 528 may alternatively be passed to the Winsock® interface 526 as IP data packets via a network driver 530 that exchanges information with a network connection 532 that may, for example, be an Ethernet, ISDN, or POTS connection.

[0059] A data manager 534 functions as a data distributor or data hub. The data manager 534 receives and interprets file data from line 536. The data manager 534 further provides an optional HTTP proxy service via line 538, uses an SDP + data store 540, and schedules data-related tuning requirements. The data manager 534 may store data files (e.g., HTML, GIF, etc.) on a local file system 541 (e.g., a hard disk) via a fifth data path 542.

[0060] The data manager 534 may use a TAPI library block 546 to communicate via a telephony application programming interface (TAPI) via line 544. The TAPI library block 546 is in direct communication with a modem 548 having a POTS phone line connection 550. In this way, the data manager 534 can report to a service provider which advertisements a particular user has viewed or selected (i.e., advertisement tracking). In addition, the data manager 534 communicates with a service/CA manager 552, which sets tuning priorities/controls, manages conditional access messages, and resolves messages relating to program tuning information that are exchanged via a third data path 554 to/from the tuner driver block 502.

[0061] The SDP + data store 540 is a database that contains all the current SDP + record information. The SDP + data store 540 passes DPG data store queries for data item description and display formatting information to a data program guide block 558 on line 556. The data program guide block 558 contains the dynamic HTML pages, including graphic content, that is currently being broadcast by the satellite communication system 100. The data program guide block 558 may retrieve files from the local file system 541 via a fourth data path 560. The SDP + data store 540 may also pass enriched TV data store queries 562 to an enriched TV function 564 that serves to map a channel to an IP address and a port. The enriched TV function 564 may further receive tuning control information, via line 566, from a tuning control interface 504 and may, accordingly, pass screen formatting information to the TV control block 504 on line 570. The enriched TV function 564 and the data program guide block 558 may exchange information with a browser application 572 along a first data path 574 and a second data path 576, respectively.

[0062] As described in section II of this disclosure, a user may interact with the PPG to invoke the download of file data (e.g., by selecting various "software" links). The PPG utilizes SDP+ records to perform this task. The SDP + records are stored in the SDP + data store 540. At the scheduled time of reception, the data manager 534, which holds schedule information, examines the records in the SDP + data store 540 to determine the multicast IP address on which the download will be broadcast. After the data manager 534 has determined the multicast IP address, the service manager 552 looks to the BARP table, which may be stored on the local file system 541, to determine tuning information for the multicast IP address found in the SDP+ record. For example, a broadcast of Quicken '98™ software may be broadcast on multicast IP address 1.2.3.4 and that multicast IP address may correspond to tuning information indicating transponder two SCID five, according to the BARP table. Once the tuning information is determined, it is passed to the service/CA manager 552, which tunes the tuner driver 502 to, for example, transponder two, SCID five.

[0063] File information received by the tuner 502 is passed to the tuner NDIS driver 522, where it is converted into IP data and passed to the Winsock® 526, via line 524. The Winsock®, in turn, passes the IP data to the data manager 534, which performs the BFDP function on the IP data to recover the data for Quicken '98™. The data associated with Quicken '98™ is stored on the local file system 541 for later use. Any data determined by BFDP to be missing from the received Quicken '98™ file will be obtained on subsequent broadcasts of the file. When the complete file has been stored on the local file system 541, Quicken '98™ is complete and ready to run.

V. Data Packets

[0064] FIG. 8 is a diagram illustrating a preferred type of transport data packet that may be transmitted via the system 100 shown in FIG. 1 and processed by the receiver station 106 shown in FIGS. 22 and 23. More specifically, the data packet may be coupled to the receiver station shown in FIG. 7 via line 510. The preferred data packet shown in FIG. 8 is in the format and of the type used in the DirecTV® digital broadcast system. As shown, each data packet may be, for example, 147 bytes long. The first two bytes (a byte is made up of 8 bits) of information contain the SCID and flags. As previously stated, the SCID (service channel ID) is a unique 12-bit number that uniquely identifies the packet's service channel. The flags are made up of four bits used primarily to control whether or not the packet is encrypted and, if encrypted, which key to use to decrypt the packet. The third byte of information is made up of a four-bit packet type indicator and a four-bit continuity counter. The next 127 bytes of information consists of the "payload" data, which is the actual usable information sent from the program provider. The payload can be any of the various types of data sent over the airlink, including video, audio, conventional program guide data, data related to the layout/format/content of the template pages of the present invention, conditional access data, webcasting data, software

download data, etc.

VI. Audio/Video Processing

[0065] The architecture shown in FIG. 7 may be used to receive audio and video signals associated with television programming. When a user desires to watch television programming, the service/CA manager 552 tunes the tuner driver 502 to the appropriate transponder and SCID or SCIDs to receive the appropriate programming signals. The received signals are passed to the MPEG video driver 506 via line 512. The MPEG video driver 506 appropriately processes the received signals to obtain audio and video signals that are passed to the video VGA driver 508, which, in turn, passes the signals to a monitor for display.

VII. Data Processing

A. Protocol Stack/Broadcast File Download Protocol (BFDP)

[0066] As discussed in section I of this disclosure, the PPG of the present invention requires the presence of appropriate data at the receiver station 106. Although a variety of data processing techniques could be used in conjunction with the PPG of the present invention, BFDP, BARP, and SDP + are exemplary of preferred data processing methods. Respectively, these methods provide a way of reliably transferring file data in a one-way communication channel, resolving IP addresses into physical addresses, and announcing to the receiver station 106 how to display available data streams for selection, and when and how to tune to data streams selected by the user.

[0067] Illustrated in FIG. 9, is a preferred data flow through a protocol stack that utilizes the BFDP, BARP, and SDP + data processing methods. The transmission station 102 (or "headend") builds transport data packets for transmission in accordance with the headend data flow arrow. There are four primary data flow paths through the protocol stack at the transmission station 102. File data begins at an application layer 602 and is passed down through a BFDP layer 604, a UDP layer 608, an IP layer 610, and is encapsulated for transmission to the receiver station 106 by an MPT layer 614 and a transport layer 616. Webcast data begins at the application layer 602 and is passed down through a webcast layer 603, the BFDP layer 604, the UDP layer 608, the IP layer 610, the MPT layer 614, and the transport layer 616. SDP+ records begin at the application layer 602 and are passed down through an SDP + layer 606, the UDP layer 608, the IP layer 610, the MPT layer 614 and the transport layer 616. BARP information begins at the application layer 602 and is passed down through a BARP layer 612, the MPT layer 614 and the transport layer 616. Transport packets received at the receiver station 106 (or "subscriber") are resolved into BARP information, SDP + records, webcast information, and file data by passing the received packets up through the protocol stack in the direction indicated by the subscriber data flow arrow.

[0068] Illustrated in FIG. 10 is an exemplary method of processing a data packet using the protocol stack shown in FIG. 9. FIGS. 9 and 10 are described is more detail below in connection with in-depth discussions regarding the BFDP, BARP, and SDP + data processing methods.

[0069] Downloading file data is especially difficult within the DTH system 100 (shown in FIG. 1) because the DTH system 100 does not provide a backchannel communication path from the receiver station 106 to the transmission station 102 (i.e., the communication path is a one-way path to the receiver station 106). The absence of a backchannel makes it impossible for the receiver station 106 to acknowledge to the transmission station 102 that a software file was completely received and error free. Additionally, the absence of a backchannel prevents the receiver station 106 from requesting rebroadcast of missing data from the transmission station 102. Although the communication channel associated with the DTH system 100 has a very low bit error rate, relatively long periods of signal interruption may occur. For example, snow or rain, either at the transmission station 102 or the receiver station 106 may cause the communication channels of the system 100 to fade, thereby causing received signal errors. Additionally, user activity, such as receiver station tuning or deactivation, may cause signal interruptions. If signal interruptions occur during the download of file data, the file data will be incomplete and inoperable.

[0070] One preferred method of addressing the difficulty associated with transmitting file data along a one-way communication path, such as that used by the PPG of the present invention, uses data carousels at the transmission station 102 that repeatedly broadcast the same file data to the receiver station 106 in conjunction with a data transfer protocol that is the subject of a co-pending, commonly assigned patent application serial no. _____ filed on _____ and entitled _____. The Broadcast File Download Protocol (BFDP) prepends a header to the file before transmission of the data packets. This header allows a download file to be reassembled from information received during one or more broadcasts of the same download file. Thus, if some file data is lost or corrupted during a first broadcast of the download file, BFDP allows the receiver station 106 to "fill in" any missing or corrupted file data with file data received during a subsequent broadcast of the same download file, thereby avoiding the constraint of having to receive an entire file without corruption/interruption during a single broadcast.

[0071] The details of BFDP will now be explained with reference to FIGS. 9 and 10. If a file (e.g., a website, a software file, etc.) is to be broadcast from the

transmission station 102 to the receiver station 106, data from the application layer 602, such as webcast, is passed to the BFDP layer 604. For purposes of explanation of the BFDP, it will be assumed that a data file 620 having 2 kilobytes (2K) of data is to be transmitted. The data file 620 is received by the BFDP layer 604, which if necessary, breaks the data file 620 into smaller data fragments 622 and 624. For purposes of explanation it is assumed that the data file 620 is split into two 1K data fragments 622, 624 and that a BFDP header 626 is prepended to each of the data fragments 622, 624. The size of the fragments is a tradeoff between overhead and the probability of data loss. If low overhead is desired, the size of the data packet will be large with respect to the BFDP header on the data. However, if the probability of data loss is high, the size of the data packets should be made small to minimize the data lost if a single packet is lost. Typically, the probability of data loss is determined by channel characteristics. The remainder of the processing for each fragment is identical. A sample format for the BFDP header 626 is shown in FIG. 11.

[0072] The eight fields of the sample BFDP header 626 provide information concerning the number and order of the data fragments 622, 624 that are broadcast to make up the data file 620. Each field in the sample BFDP header 626 is represented by four bytes, except for filename, which is represented by sixty-four bytes. The Sync. field contains information that may be used to assist in identifying the header. An ID field is a representation of the object ID for the file being broadcast. The object ID may be used for data filtering at the receiver station 106. The Version field indicates the version of the BFDP used to create the present packet. Filename is sixty-four bytes of information used to indicate the filename and path where the data fragment is to be stored on the receiver station 106 (e.g., C:\downloads\xyz). Preferably, the filename field is used only for special files and is not generally used. For example, when webcast information is transferred, a HTTP header is used and the filename field is ignored. The Modified field denotes the last time the fragment was modified. Preferably, this representation is in UNIX time_t format. Count, Number, and Size fields refer to the number of fragments used to make up the original file data that is broadcast, the number of this fragment, and the size of this fragment, respectively. The count, number, and size fields are key pieces of information that allow BFDP to reconstruct a complete data file from multiple broadcasts of the data file. For example, a data file may be broken into 10 fragments and, during transmission, fragments 1-5 and 8-10 were received by the receiver station 106. On subsequent broadcasts of the data file, the receiver station 106 examines all of the BFDP headers on the received fragments and only stores the data packets indicated as fragments 6 and 7 in their BFDP headers, thereby filling in the received data file.

[0073] As shown in FIGS. 9 and 10, after the processing is complete at the BFDP layer 604, the resulting data packet is transferred to a UDP layer 608, which prepends a UDP header 628 to the packet. The UDP header 628, which is standard and well known in the art, is shown in FIG. 12. The UPD header 628 includes fields that denote source and destination ports for the data. That is, UDP header fields contain information indicating the application that is providing the data (source port) and the application that is to receive the data (destination port). At this point in the processing, the data packet is referred to as a UDP packet 630.

[0074] Data transferred to a computer through a connection is typically in an Internet protocol (IP) format, which is well known to those skilled in the art. Accordingly, the UDP packet 630 is passed to the IP layer 610, which in a well known manner, prepends an IP header 632 onto the UDP packet 630, thereby creating an IP packet 634. The IP header 632, which is shown in FIG. 13 denotes, inter alia, the IP addresses of the data source and destination computers. Information that is broadcast to a number of users preferably uses a multicast IP address. Alternatively, information may be addressed to specific users via a standard IP address.

[0075] After the UDP packet 630 has been properly processed by the IP layer 610 to create the IP packet 634, the IP packet 634 is passed to an MPT layer 614. The MPT layer 614 processes the IP packet 634 to create an appropriate number of MPT packets 636. For example, in digital video broadcasts (DVB) the size of the MPT packets may be 185 bytes. Alternatively, the MPT packets may be 127 bytes long for other direct to home (DTH) applications. For use in the present system 20, each the MPT packets 636 is 127 bytes long including a header and data. The MPT layer uses a number of packet configurations, shown in FIGS. 14A - 14D, to create the 127 byte packets. If the IP packet 634 contains 114 bytes or less, only one MPT packet referred to as an "Only Packet" 760 needs to be created. The preferred format of the Only MPT packet 760 is shown in FIG. 14D. The Only packet 760 includes: a six bit flag field that is preferably reserved and set to all zeros, a one bit start of frame (SOF) field that indicates that this packet is the start of the frame, a one bit end of frame (EOF) field that indicates that this packet is the end of the frame. If the IP packet 634 contains 114 bytes or less, only one MPT packet 636 will be sent, therefore the Only packet header indicates that the Only packet 760 is the start of the frame and the end of the frame. The Only packet 760 may also include a field indicating the sub-SCID address of the packet, which preferably includes a two byte type code and a four byte type-dependent code. Preferably, the type code is 0x0100, which signifies that the last four bytes are the multicast group address to which this frame belongs. The Only packet 760 may also include a frame type field, which identifies the type of content in the MPT frame. Preferably, this field is used to indicate whether the frame is an

IP frame or a BARP frame. Preferably, the frame type field is filled using Internet Assigned Number Authority (IANA) standard numbers. Further, the Only packet 760 may include a cyclic redundancy check (CRC), which is a 32-bit number computed over the entire MPT frame.

[0076] If the IP packet 634 is to be processed by the MPT layer 614 is longer than 114 bytes, Start 730, Middle 740, and End 750 MPT packets shown in FIGS. 14A - 14D are preferably used to process the IP packet 634. The headers of these packets use all combinations of the fields described in conjunction with the Only packet 760. As shown in FIG. 10, the first 118 bytes of the IP packet 634 are loaded into the MPT Start packet 730. The start header of the MPT packet denotes a MPT packet as the start of the frame by setting the SOF bit. If the IP packet 634 is larger than 244 bytes the appropriate number of Middle packets 740 will be filled with 126 byte sections of data from the IP packet 634. The SOF and EOF bits will not be set because the MPT packet is a middle packet. Numerous middle packets will be filled with the IP data until there is less than 122 bytes of data remaining in the IP packet 634. At this point an End packet 750, is filled with the last bytes of information and appended with a CRC. This method of using Only, Start, Middle, and End packets yields MPT packets that are all exactly 127 bytes long.

[0077] After each IP packet 634 has been converted to one of the MPT packets 636, each of the MPT packets 636 is passed to the transport layer 616. The transport layer 616 places each 127 byte packet into the 127 byte payload section of a transport data packet (shown in FIG. 8). The complete transport data packet is passed to the uplink frequency converter 118 of FIG. 1 and broadcast to the receiver station 106.

[0078] As the receiver station 106, which is tuned to a particular transponder and SCID, receives packets of information, the data packets traverse up through the protocol stack as indicated by the subscriber data flow indicated on FIG. 9. The transport layer removes the payload from each transport packet. After the appropriate processing, the payload is passed to the MPT layer 614, which strips the MPT header from the packet and assembles all relevant data from MPT packets to assemble the IP data frame. The IP layer 610 strips the IP header 632 from the data, performs well-known IP processing functions, and routes the data to the UDP layer 608. The UDP layer 608 strips off the UDP header 628 and routes the remaining information to the proper application (port) as denoted by the UDP header. The BFDP layer 604 strips the BFDP header 626 from the data packets and, using the information in the headers, reassembles the data contained in the BFDP packets into the data file 620 as sent by the transmission station 102. Additionally, if necessary, the receiver station 106 denotes missing data packets through examination of the BFDP headers. Thus, the PPG of the present invention may reassemble the original data file in accordance with the BFDP header fields at the receiver station 106 after multiple broadcasts of the original data file. That is, any missing data after the data is broadcast will be "filled in" with the appropriate data from subsequent broadcasts of the original data a file. For example, if a 1 megabyte (MB) file is broadcast and the receiver station 106 successfully acquires all but 1 kilobyte (KB) of the broadcast information, instead of having to reacquire all of the data that the receiver station 106 has already received, the receiver station 106 simply waits for and acquires the 1KB of data that it needs to complete the 1 MB file.

B. Broadcast Address Resolution Protocol (BARP)

[0079] As referenced earlier, the broadcast address resolution protocol (BARP) layer 612 is required to resolve IP addresses into physical (i.e., satellite transport) addresses. BARP is the subject of a co-pending commonly assigned application entitled _____, filed on _____ and bearing serial no. _____/_____. The BARP layer is coupled to the MPT layer 614 and is used to map a multicast source IP address to transport-specific tuning information. That is, BARP is a map that tells a receiver station 106 on which transponder or transponders and SCID or SCIDs, information from a particular source IP address may be found. For example, when a user selects information from the PPG, the receiver station 106 uses BARP to determine tuning parameters (e.g., transponder and SCID) for the information selected by the user. Preferably, BARP information is periodically sent on as many transponders as possible so that users have easy access to the most current BARP information.

[0080] BARP consists of a header followed by zero or more address records. BARP preferably uses MPT frame type 0x0806. FIGS. 15A and 15B represent the format of a BARP header and a BARP address record, respectively. The BARP header includes version, change number, record count and reserved fields. In this example, version is a 1 byte field that represents the version of the BARP format used to create the header and address record. Change number is a 1 byte field that is incremented each time anything in the header or any of the address records change. Record count is a 2 byte field that indicates the number of address records that follow this BARP header. The reserved field is a four byte field that may be used to provide system flexibility in the future.

[0081] The BARP address record, as shown in FIG. 15B, includes six fields. An IP address field contains a four byte representation of an IP address. Transponder is a bitmap field identifying the transponders on which the previously-noted IP address can be found. Each bit in the transponder field corresponds to a transponder. Set bits in the transponder field indicate the presence of the IP address on that transponder. For example, if the first bit is set (1) and the rest of the bits are clear (0) then

the IP address listed in the IP address field is present only on the first transponder of the system. The SCID field denotes the 12 bit SCID that contains the information provided by the IP address listed in the first field of the header. Preferably, the four most significant bits are reserved. Channel is 10-bit channel number that is associated with the this SCID and transponder. For example, transponder two, SCID nine may correspond to channel 105. Preferably, the most significant 6 bits of the channel field are reserved for future use. Service type is the type and paradigm of the channel associated with the transponder and SCID in the address record. The reserved field is 3 bytes long and is preferably reserved for future system use. Information for channel and service type fields are preferably supplied by the broadcaster to satisfy tuning requirements of subscriber units.

[0082] While the BARP and BFDP protocol layers represent one preferred way of transmitting the information related to the PPG of the present invention, other transmission systems and methods may be substituted without departing from the spirit of the invention.

C. SDP+ Records

[0083] Another difficulty faced in utilizing the wide variety and large amount of information transmitted within the DTH system 100 is providing a way for the PPG to efficiently find and process the various kinds of data that are available at various times within the multiprogram data stream. One preferred method that allows the PPG of the present invention to efficiently find and process information for presentation to a user are "session description protocol plus" (SDP+) records. SDP+ records are the subject of a co-pending commonly assigned application entitled _____, filed on _____ and bearing serial no. _____/_____.

[0084] An SDP + record is an announcement mechanism that includes a number of fields, which are assembled into a single record or file to provide information on available services such as webcasts, downloads, and streaming data or other services. The SDP + protocol is a combination of standard SDP fields and augmentations, or extensions, to the standard SDP protocol. Additional details regarding the standard SDP protocol may be found in RFC 2327. The standard fields of the SDP protocol that are used in the of the SDP + protocol include, protocol version, the owner/creator and session identifier (i.e., the IP address of the creator of the SDP record), the name of the SDP session (i.e., the name of the SDP record), a brief description of the session (i.e., what the SDP record is for), the multicast address on which the session is being broadcast, the start and end times of the broadcast, the repeat times of the broadcast, a list of Internet webpages that can provide additional information on the item that is going to be broadcast, what the port of the broadcast is (i.e., the UDP port of the broadcast), the type of broadcast (e.g., BFDP, Stream, Webcast or Intercast), sorting and filtering information.

[0085] As noted, an SDP + record may also contain information such as the time a particular service will be broadcast, the multicast IP address on which the service will be broadcast, the size of the file that will be broadcast, and information relevant to the PPG such as text or images that should be displayed to the user. Each download service (e.g., each webcast, each software download, etc.) has its own SDP+ record, which is broadcast to all subscribers to inform them of the information that is available for download. With reference to PPG information, SDP + records are used by the PC 128 to build particular sections of pages using selected information resident within the PC 128 (e.g., the basic page templates shown in FIGS. 2-5) and selected dynamic data that is received from a satellite in the form of SDP + records. When the user launches the interface into another state or page, the PPG builds the destination page as instructed by the templates and by the SDP + records. The page is then displayed on the user's PC monitor 130.

[0086] SDP + records also allow users to pre-select download content from descriptions of the content, then filter for that information as it arrives in the one-way data stream of the DTH system 100. The descriptions of the content may include extended SDP records including protocol version, name, times of broadcast, IP address, mandatory download status, ID number, run command, category, file size, text messages, channel, images, keywords, etc.

[0087] As previously mentioned, SDP + records also provide announcement information including content type, start time, duration, Internet address information, and actions to be taken on receipt of the information. Announcement management is critical to finding the data stream, discrete download or webcast information in the received transmission. SDP + records can be rescinded and modified, once they are present on the user's PC 128. SDP+ records can be used to indicate mandatory download events such as software updates. The system user (client) uses SDP + records to schedule program reception. After the client makes selections based on the SDP + record information, the receiver station 106 properly tunes itself to receive the selected information.

[0088] SDP + records are a combination of conventional SDP records and extensions to the conventional SDP records. Generally, the extensions to the standard SDP protocol consist of fields for linking different download services together, specifying if a download file is mandatory, archived or should be run upon download to the receiver station 106. The extensions also provide for specification and placement of graphics for the PPG, the notification of the user upon receipt of the SDP + record, and the recission of previously sent SDP + records. These unique extensions coupled with the

standard SDP protocol yield the SDP + protocol used in conjunction with the PPG of the present invention. The details of the conventional SDP fields and the unique extensions of the present invention are best described in conjunction with the exemplary SDP+ records shown in FIGS. 16A-16D.

[0089] Referring now to FIGS. 16A-16D, fields indicating version (v), record ID (o), multicast IP address (c), time (t), and port (m) are required for all SDP+ records of any kind. Additionally, for any BFDP download the object ID BFDP code (a=key:) is needed. The run command (a = run:) is required for all streaming data downloads. For all streams having an entry in the MPG a channel link (a = channel) is required. Additionally, for all webcasts a URI address field (u = ⟨uri⟩) is required.

[0090] FIG. 16A is a sample SDP + record for streaming data, which is commonly referred to as a ticker. The field "v = 0" refers to the version of the SDP + protocol used to produce this SDP + record. The record ID, which is represented by "o," indicates the unique session ID for this particular record. Specifically, the session ID for this SDP+ record is 0001 and the version of this record is 17. The session ID is a way to refer to this particular SDP + record and 17 indicates that there have been 16 previous versions of this SDP + record before this version. The name of this session is represented by "s=Announcement Dump." However, it should be noted that the session name is arbitrary ASCII text that is used to identify the SDP + record. The field "c" represents the multicast IP address of this session and "/1" indicates that the Time To Live (TTL) value, which indicates the number of "hops" that a packet may make before it expires. Multicast IP addresses denote the IP address on which the information corresponding to the SDP + record will be broadcast. The multicast IP address is used in conjunction with the previously described BARP table to tune a subscriber's receiver station 106 to the appropriate transponder and SCID to receive the broadcast information. When a user makes a request to receive broadcast information using the PPG, the receiver station 106 determines the multicast IP address on which the information will be broadcast by looking to the SDP + record corresponding to the selection. Once the multicast IP address is determined, the receiver station 106 uses the BARP table to correlate the multicast IP address to a transponder and SCID. The receiver then appropriately tunes itself to the proper transponder and SCID to receive the broadcast information. Since streaming data or tickers are always running, the start and end times represented by "t = 0 0" indicate that the data service is constantly running and is permanent. The field "m =" indicates that the UDP port of the data is 3278 and the type of data is streaming data.

[0091] The SDP+ record shown in FIG. 16A includes "a=key:1," which indicates that the object ID for this SDP + record is 1. The object ID may be used for sorting or other functions. The object ID in the SDP + record matches the object ID sent in the BFDP header. The field "a = run: consoleticker" indicates that when the download is complete, an executable file named consoleticker should be started. The standard SDP field "a = keywds" is used to correlate SDP records to one another. For example, in the SDP + record shown in FIG. 16A "tsetup" is used to correlate this SDP + record with another SDP + record, such as a client download file.

[0092] FIG. 16B is an example SDP+ record for a file download. Similar to the ticker SDP+ record of FIG. 16A, the file download SDP+ record a file download specifies the version of the SDP + protocol used to produce the SDP + record, the record ID, the name of the session, the multicast IP address of the session, and the object ID of the session. Additionally, the SDP+ record shown in FIG. 16B specifies download times using a "t= 3079382400 3155745600," wherein the first number is the start time of the broadcast and the second number is the end time of the broadcast. The start and end times are specified in decimal network time protocol (NTP) format. The "r = 10m 10m 0" specifies the broadcast repetition of the broadcasts, wherein the first number indicates the interval between broadcasts, the second number indicates the duration of the broadcasts and the third number indicates the time offset between the broadcasts. The field "m = " indicates that the UDP port of the data is 3335 and the type of data is BFDP data. The SDP+ record shown in FIG. 16B further specifies the size of the file that is to be downloaded using the "a =fsz" command. The example file download SDP+ record specifies a file size of 980K. The file download SDP + record also specifies that this file is a mandatory download using the command "a = mandatory." That is, the receiver station must receive the data broadcast corresponding to this SDP + record during one of the broadcast times. The field "a = run:cataloginstall.exe" specifies that after the data associated with the SDP + record is received, the file cataloginstall.exe must be executed.

[0093] FIG. 16C is an example of an SDP+ record that is used to specify information pertinent to a webcast. In addition to using the fields previously described in conjunction with the file download and ticker SDP + records, the webcast SDP + record may use the session description field denoted as "i = ." This field is an ASCII text field that may be used to describe the content of a particular session or webpage. The session description field may be used as the program preview description represented as horizontal lines in a child window (not shown) that may pop-up when the system pointer rolls over a video image representing a program. Alternatively, the session description field of the SDP + record may be used in conjunction with SDP + records other than webcast SDP + records. The webcast SDP + record also includes a field denoting the URI of the webpage that is broadcast. The webcast SDP + record also

uses the standard SDP extension "a = cat," which is used for sorting and filtering the SDP + records.

[0094] The webcast SDP + record uses the unique extension "a = display:type =" to indicate how the information content from the webcast will be displayed to the user. Additionally, the unique SDP+ field "a = img" is used to associate an image file (in this case cnn.gif) with a webcast. This image may be used as a thumbnail or any other representation of the content of the webcast. The image field and the display type field can work together to provide information for the PPG. Display type may be used to indicate on which page of the PPG the image specified in the image field must be placed. For example, type may be used to specify Movies, Sports, New, Data, or any other available category, each of which may be represented by a number. As shown in FIG 16C, type = 1 is specified, which may correspond to Movies. Accordingly the image cnn.gif will be placed on an appropriate page of the PPG as shown in FIG. 2. The specification of priority =8 denotes the particular location in which the cnn.gif image will be placed on the page. Referring to the movies page shown in FIG. 2, different priorities correspond to different locations in the arrangement of the images within the video/picture segment.

[0095] FIG. 16D is an example of an SDP + record that may be used to represent enriched TV. In addition to the field discussed in conjunction with the SDP + records, this SDP + record includes the field "a = channel." This field contains a 32-bit channel number that associates the data contained in the enriched video to channel content of a channel located in the program guide. The information contained in the enriched TV may be associated through a number of program guide channels.

D. Webcast

[0096] As previously noted, the DTH system 100 broadcasts discrete downloads. These downloads are data items that have well-defined broadcast schedules and require detailed announcement information to locate the items in the received data. Examples of discrete downloads include software applications, such as spreadsheets, word processors or games. Webcasting is a special case of the discrete download. A webcast is an ongoing and repeating download of specially selected web content. The content is usually grouped by domain. Minimal scheduling is required for downloading webcast information. Multiple groups of content may be identified by the same identifier, thereby creating a one-to-many relationship among the items of interest. The system 100 may archive webpages pages on a the PC 128 for later viewing.

[0097] As webpage information is received by the subscriber unit it is stored for later use. In the preferred embodiment, webpage information is received in a compressed format and is stored directly (i.e., without extraction) by the subscriber unit. Preferably, the present invention uses an archiving scheme based on the PKWare™ PKZIP™ format. However, other alternative archiving formats may be used. If the archived files are compressed, the files are preferably extracted on demand using a PKWare™ extractor. If, however, the files are not compressed, any ZIP extractor may be used to extract and view the files. Preferably, the filenames used in the webcast archive are actually the uniform resource identifier (URI).

[0098] Preferably, webcast archive files have a dedicated filename extension. On any given data carousel, the contents of which is repeatedly broadcast, there must be exactly one main file for each webcast. Preferably, this file contains a snapshot of the entire website or website subset as selected for broadcast. Update archive files may be used to replace portions of the main file on the carousel. The subscriber unit stores all archive files in a subdirectory corresponding to the session ID of the webcast. Preferably, when a main file is received that is newer than the current main file in that directory, all other files in that directory will be removed and any links in the proxy server's cache map file for this webcast will be replaced with the URIs in the new main file.

[0099] In accordance with the present invention, the subscriber unit preferably maps uniform resource locators (URIs) to archive files. The map allows the subscriber unit to locate the archive file containing a URI that the user desires to view. When the subscriber unit receives the main file, the subscriber unit removes all files and cache map file links to the associated session prior to the receipt of the new main file. When the user requests a webpage, the subscriber unit extracts and decompresses the appropriate archive file data to a socket. This extraction is done in real time rather than extracting the entire archive file to disk. The subscriber unit also preferably has the capability to save partially downloaded files and acquire missing portions of the files on the next broadcast of the files as with all BFDP deliveries.

[0100] In accordance with the present invention, the headend unit is capable of manipulating the archived files using functions that archive files, determine the number of files in an archive file, return the name of a particular entry in an archive file, remove entries from an archive file, and merge a number of archive files into one archive file. The function that puts entries into an archive file includes a field denoting the file or files to be archived. Preferably, wildcard indicators may be used to specify a number of filenames for entry into the archive file. The archive function also preferably allows for a specification of a location to which the archive file should be written (e.g., a path name). In a preferred embodiment the archive function allows for specification of compression or no compression for the archived file. The archive function parses the specified files, reads the hypertext transport protocol (HTTP) header, and

archives the specified files to an output file using the URI found in the HTTP header.

[0101] A function that counts the number of files in an archive is also preferably implemented at the head-end unit. This function allows for a specification of an archive filename and returns the number of files stored in the archive file. Another desirable function is that of a function that returns the name of a file located in an archive file. This function allows for specification of an archive filename, the index or location of the file in question, the name of a buffer that will be filled with the name of the file in question, and the size of the specified buffer. Based on the inputs specified this function preferably returns the name of the file located in the specified index position in the specified archive file, the size of the file, and the length of the character string returned in the buffer size.

[0102] A function that erases portions of an archive file is also desirable. This erasing function allows for the specification of the archive file in question, the array index or indices to be erased from the archive file, and the number of elements specified in the index or indices to be erased. Preferably, a function is included that allows for the merging of two archive files. This merging function allows for the specification of two archive file names. One of the archive filenames is the file that is to be merged into the archive file bearing the other specified filename.

VIII. Conclusion

[0103] Of course, it should be understood that a range of changes and modifications can be made to the preferred embodiment described above. It is therefore intended that the foregoing detailed description be regarded as illustrative rather than limiting and that it be understood that it is the following claims, including all equivalents, which are intended to define the scope of this invention.

Claims

1. A computer based graphical user interface for facilitating the selection and display of transmitted audio, video, and data, comprising:

   an active video segment adapted to display a currently tuned program;
   a category segment listing various categories of programs or services available for viewing;
   a video/picture segment having a plurality of video/picture areas associated with the category segment, wherein selection of a one video/picture area invokes the interface to command a receiver to tune to a particular program or service associated with the one video/picture area and to display the particular program in the active video segment; and
   a graphic/link segment, wherein selection of a graphic/link invokes a function associated with the graphic/link.

2. The interface of claim 1, wherein the graphic/link segment includes a web graphic/link indicating that there is a web page related to at least one video/picture area from the plurality of video/picture areas.

3. The interface of claim 1, wherein the graphic/link segment includes grid-guide links that invoke the interface to display a program grid-guide.

4. The interface of claim 1, wherein the graphic/link segment includes video-clip links that invoke the display of video clips in the video/picture segment.

5. The interface of claim 1, wherein the graphic/link segment includes software links that invoke the download of software to the receiver.

6. The interface of claim 1, wherein the graphic/link segment includes software links that invoke the display of a data catalog that provides a schedule of when particular computer programs/web pages will be broadcast and available for download to the receiver.

7. The interface of claim 1, wherein the graphic/link segment includes links that invoke the purchase and display of a pay-per-view program.

8. The interface of claim 1, further comprising a page segment, whereby a user may select from one or more pages associated with a particular category.

9. The interface of claim 1, further comprising a time line associated with one or more of the video/picture areas.

10. The interface of claim 1, wherein the categories within the category segment listing include at least one from the group of categories consisting of movies, sports, news, kids & family, shopping, music, educational, entertainment, and favorites.

11. The interface of claim 1, wherein the video/picture segment has six 3:4 aspect ratio video picture areas.

12. The interface of claim 1, further including one or more auxiliary display areas.

13. A method for facilitating the selection and display of transmitted audio, video, and data, comprising:

    displaying in a category segment a listing of the

various categories of programs available for viewing;

displaying in an active video segment a video/service channel to which a receiver is currently tuned;

displaying a graphic/link segment containing a least one graphic/link that invokes a feature or service associated with the graphic/link;

displaying a video/picture segment having a plurality of video/picture areas associated with the category segment;

receiving an input from a user, the input being a selection of a one video/picture area selected from the plurality of video/picture areas;

commanding a receiver to tune to a particular program or service associated with the one video/picture area; and

displaying the particular broadcast program in the active video segment.

14. The interface of claim 13, wherein the graphic/link segment includes a web graphic/link indicating that there is a web page related to at least a one from the plurality of video/picture areas.

15. The interface of claim 13, wherein the graphic/link segment includes grid-guide links that invoke the interface to display a program grid-guide.

16. The interface of claim 13, wherein the graphic/link segment includes video-clip links that invoke the display of video clips in the video/picture segment.

17. The interface of claim 13, wherein the graphic/link segment includes software links that invoke the download of related software to the receiver.

18. The interface of claim 13, wherein the graphic/link segment includes software links that invoke the display of a data catalog that provides a schedule of when particular computer programs/web pages will be broadcast and available for download to the receiver.

19. The interface of claim 13, wherein the graphic/link segment includes links that invoke the purchase and display of a pay-per-view program.

20. The display of claim 13, further including the step of displaying a page segment, whereby a user may select from one or more pages associated with a particular category.

21. The display of claim 13, further including the step of displaying a time line associated with one or more of the video/picture areas.

22. The interface of claim 13, wherein the categories within the category segment listing include at least one from the group of categories consisting of movies, sports, news, kids & family, shopping, music, educational, entertainment, and favorites.

23. The interface of claim 13, wherein the video/picture segment has six 3:4 aspect ratio video picture areas.

24. The interface of claim 13, further including the step of displaying one or more auxiliary display areas.

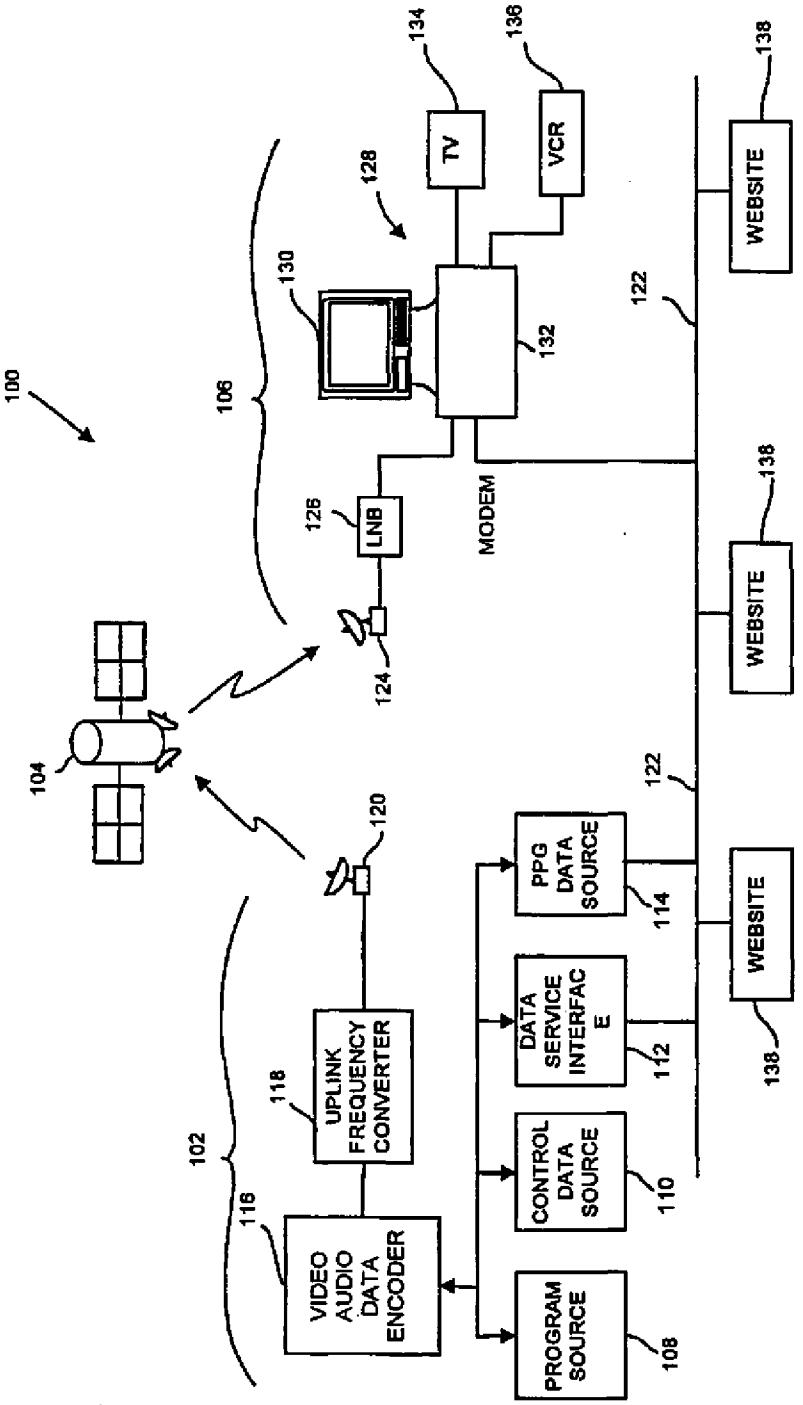

100
102
104
106
108
110
112
114
116
118
120
122
124
126
128
130
132
134
136
138
PROGRAM SOURCE
VIDEO AUDIO DATA ENCODER
CONTROL DATA SOURCE
DATA SERVICE INTERFACE
PPG DATA SOURCE
UPLINK FREQUENCY CONVERTER
LNB
MODEM
TV
VCR
WEBSITE
WEBSITE
WEBSITE
WEBSITE

FIG. 1

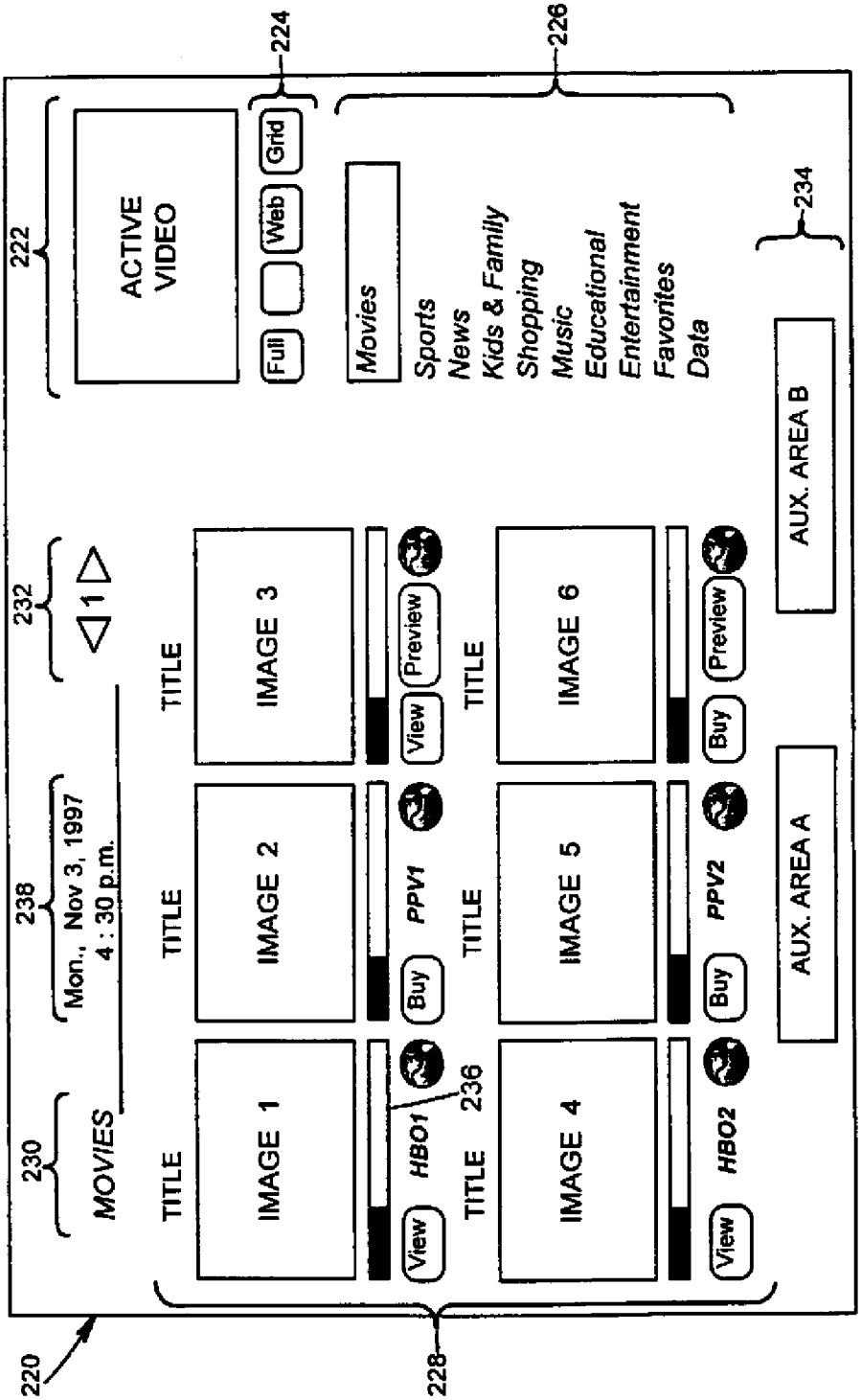

220
228
230
MOVIES
238
Mon., Nov 3, 1997
4 : 30 p.m.
232
1
222
ACTIVE VIDEO
224
Full
Web
Grid
226
Movies
Sports
News
Kids & Family
Shopping
Music
Educational
Entertainment
Favorites
Data
234
AUX. AREA B
AUX. AREA A
TITLE
IMAGE 1
IMAGE 2
IMAGE 3
IMAGE 4
IMAGE 5
IMAGE 6
View
HBO1
Buy
PPV1
Preview
HBO2
PPV2
236

FIG. 2

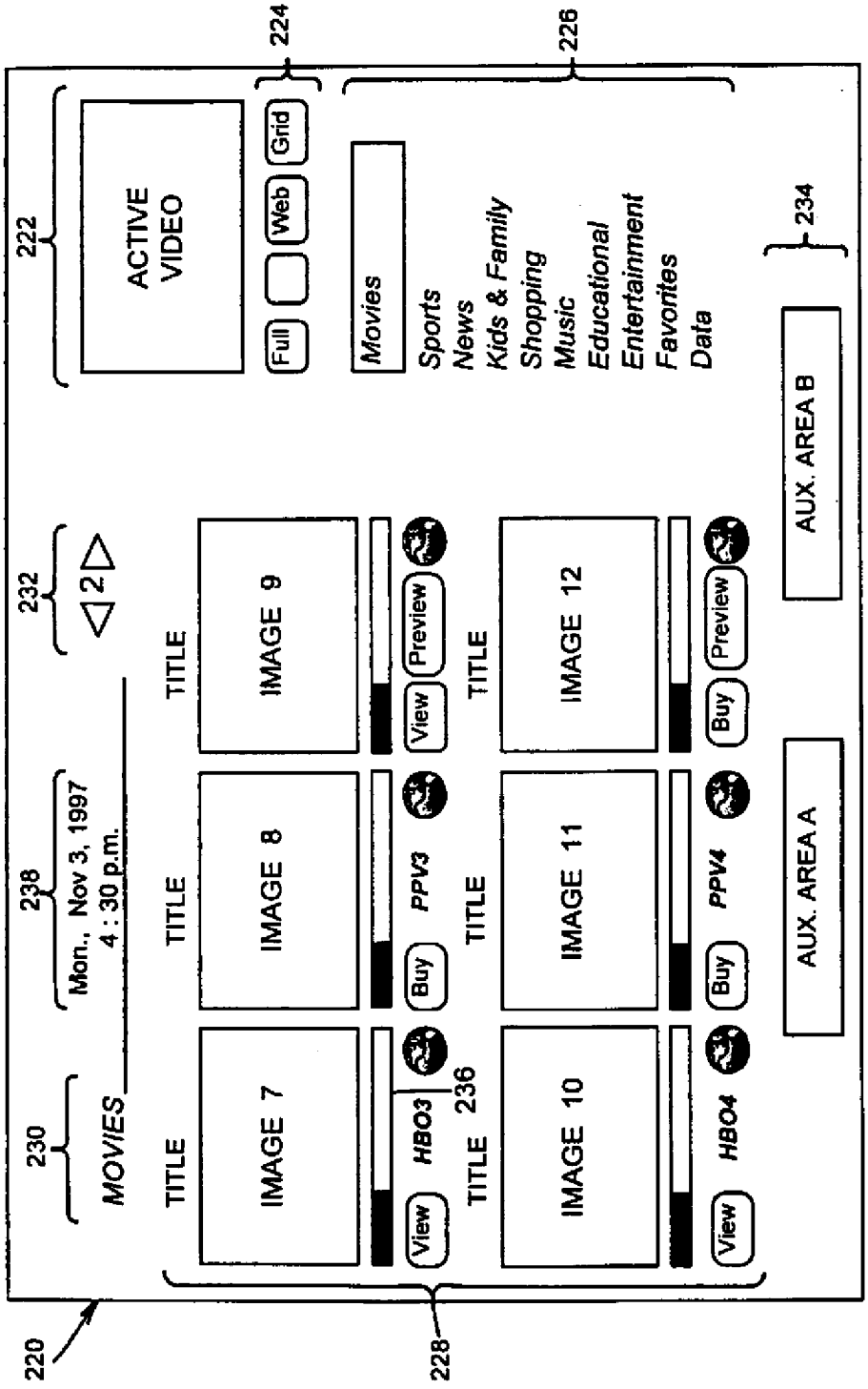

220
228
230
MOVIES
238
Mon., Nov 3, 1997
4 : 30 p.m.
232
2
222
ACTIVE VIDEO
224
Full
Web
Grid
226
Movies
Sports
News
Kids & Family
Shopping
Music
Educational
Entertainment
Favorites
Data
TITLE
IMAGE 7
View
HBO3
236
Buy
PPV3
TITLE
IMAGE 8
TITLE
IMAGE 9
View
Preview
TITLE
IMAGE 10
View
HBO4
TITLE
IMAGE 11
Buy
PPV4
TITLE
IMAGE 12
Buy
Preview
AUX. AREA A
AUX. AREA B
234

FIG. 3

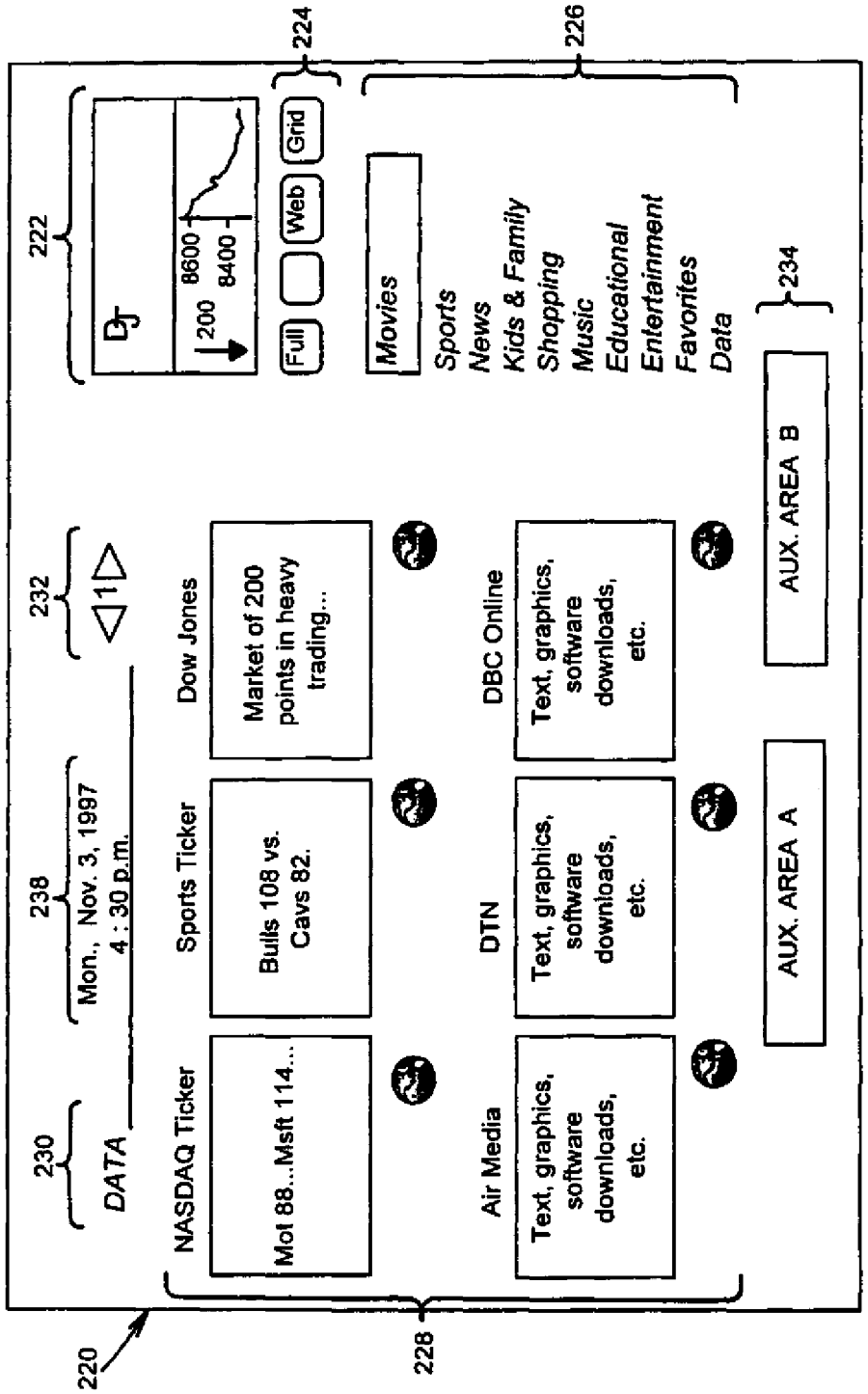

220
228
230
DATA
238
Mon., Nov. 3, 1997
4 : 30 p.m.
232
1
222
224
226
234
NASDAQ Ticker
Mot 88...Msft 114...
Sports Ticker
Bulls 108 vs.
Cavs 82.
Dow Jones
Market of 200
points in heavy
trading...
Air Media
Text, graphics,
software
downloads,
etc.
DTN
Text, graphics,
software
downloads,
etc.
DBC Online
Text, graphics,
software
downloads,
etc.
AUX. AREA A
AUX. AREA B
200
8600
8400
Full
Web
Grid
Movies
Sports
News
Kids & Family
Shopping
Music
Educational
Entertainment
Favorites
Data

FIG. 4

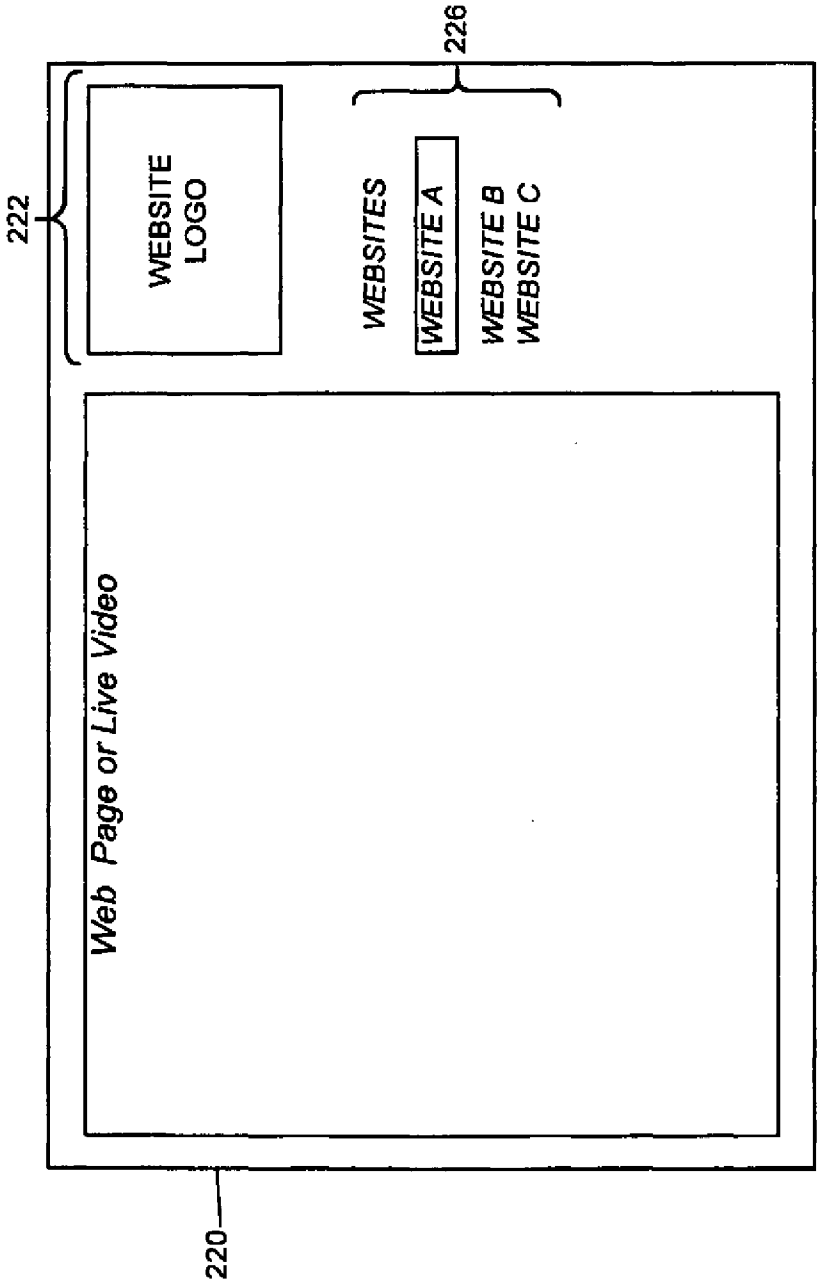

222
WEBSITE LOGO
226
WEBSITES
WEBSITE A
WEBSITE B
WEBSITE C
Web Page or Live Video
220

FIG. 5

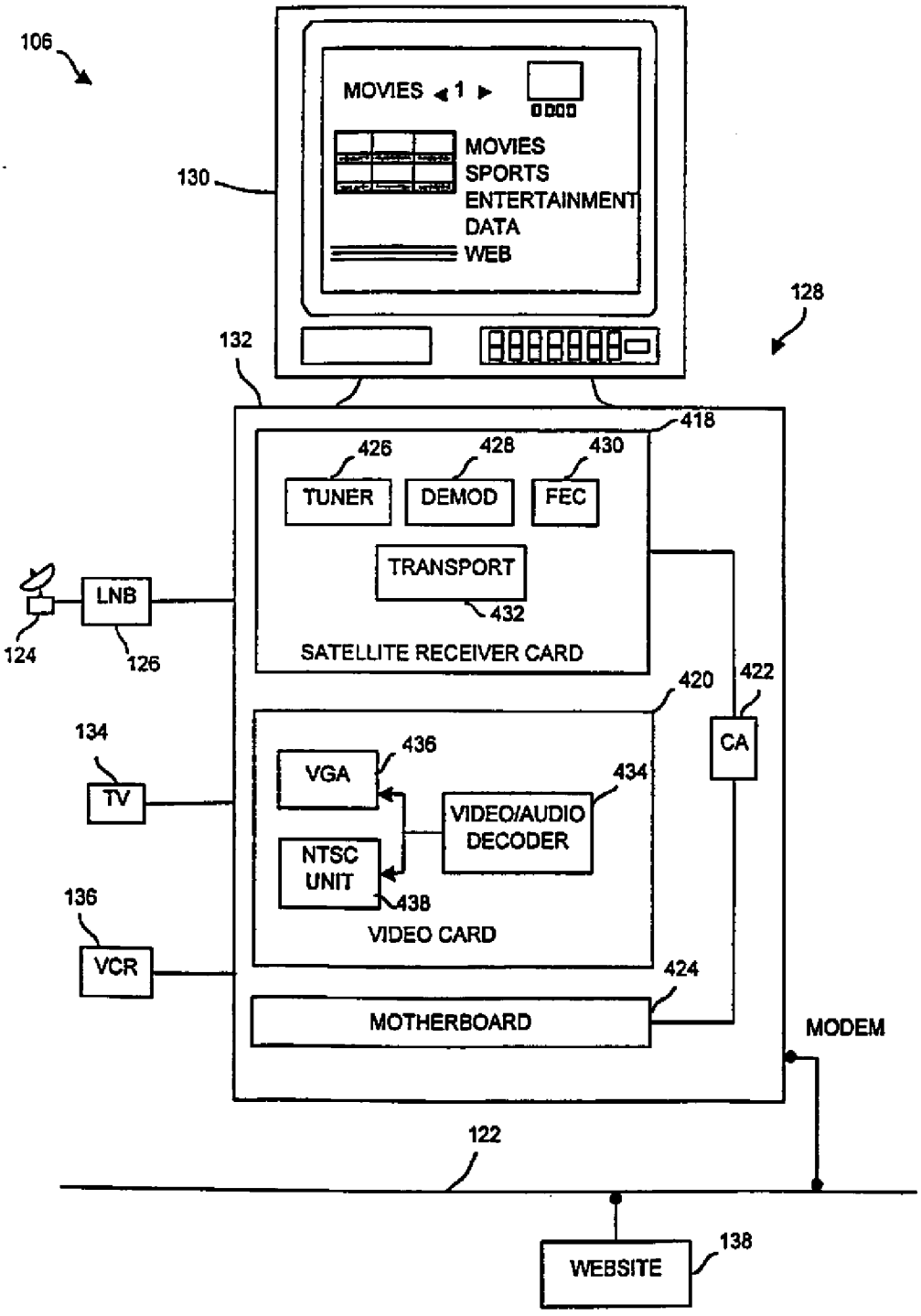

106
MOVIES ◄ 1 ►
MOVIES
SPORTS
ENTERTAINMENT
DATA
WEB
130
128
132
418
426
428
430
TUNER
DEMOD
FEC
TRANSPORT
432
SATELLITE RECEIVER CARD
LNB
124
126
420
422
CA
134
TV
436
VGA
434
VIDEO/AUDIO DECODER
NTSC UNIT
438
VIDEO CARD
136
VCR
424
MOTHERBOARD
MODEM
122
WEBSITE
138

FIG. 6

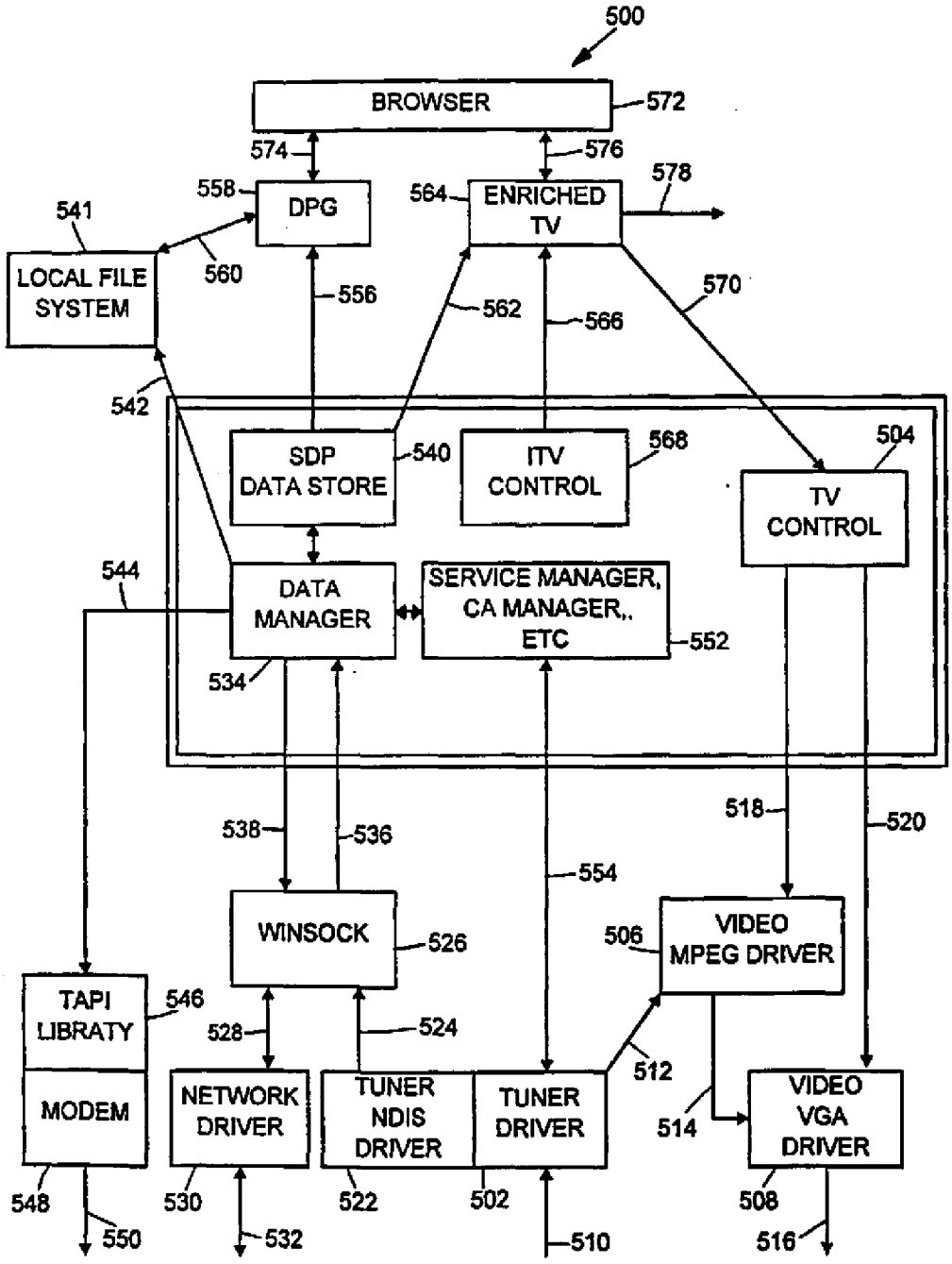

500
BROWSER
572
574
576
578
558
DPG
564
ENRICHED TV
541
LOCAL FILE SYSTEM
560
556
562
566
570
542
SDP DATA STORE
540
ITV CONTROL
568
504
TV CONTROL
544
DATA MANAGER
SERVICE MANAGER, CA MANAGER,.. ETC
552
534
538
536
518
520
554
WINSOCK
526
506
VIDEO MPEG DRIVER
TAPI LIBRATY
546
528
524
512
MODEM
NETWORK DRIVER
TUNER NDIS DRIVER
TUNER DRIVER
514
VIDEO VGA DRIVER
548
550
530
532
522
502
510
508
516

FIG. 7

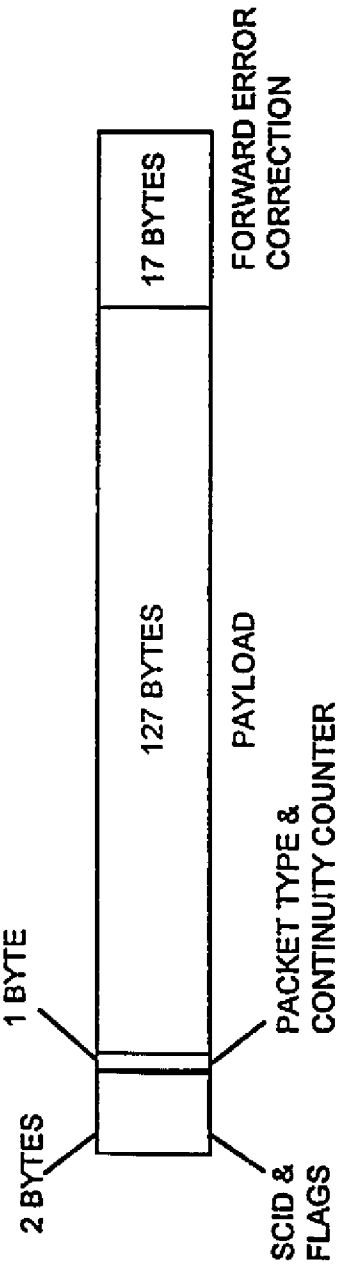

17 BYTES
FORWARD ERROR CORRECTION
127 BYTES
PAYLOAD
1 BYTE
PACKET TYPE & CONTINUITY COUNTER
2 BYTES
SCID & FLAGS

FIG. 8

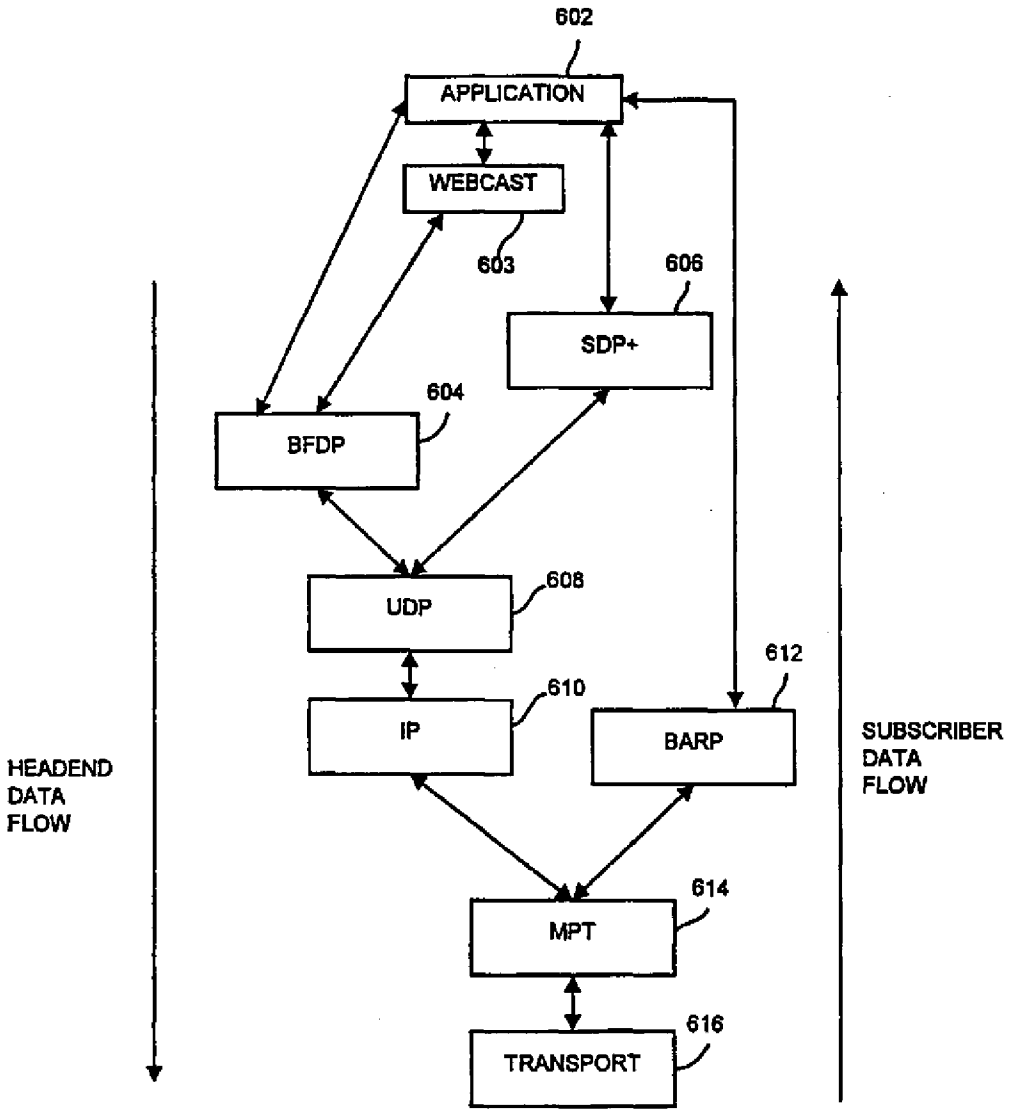

602
APPLICATION
WEBCAST
603
606
SDP+
604
BFDP
608
UDP
612
610
IP
BARP
614
MPT
616
TRANSPORT
HEADEND
DATA
FLOW
SUBSCRIBER
DATA
FLOW

FIG. 9

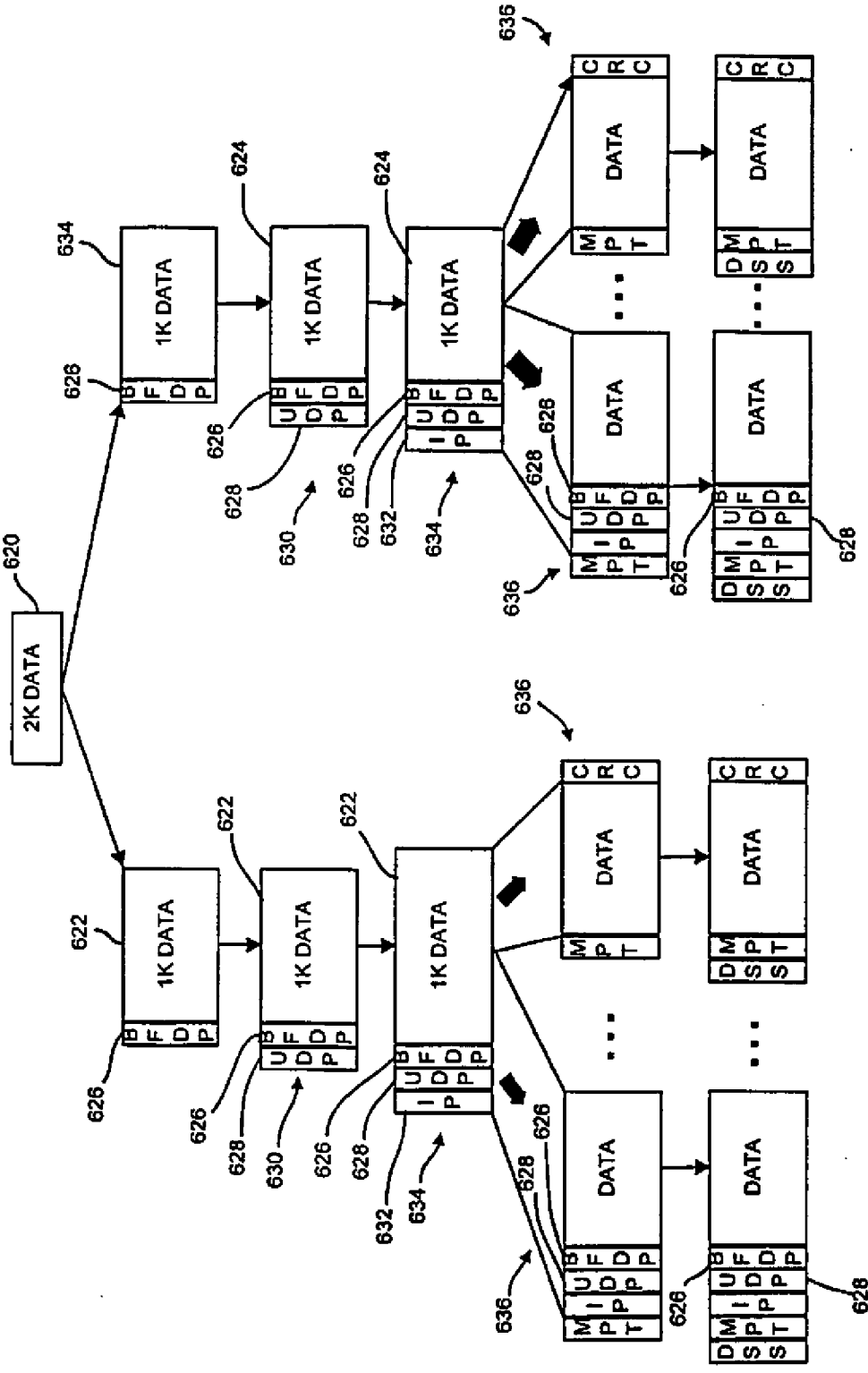

2K DATA
620
1K DATA
622
624
626
628
630
632
634
636
DATA
B F D P
U F D P
I P P
M P T
C R C
D M S P S T

FIG. 10

BFDP Header 626

Sync.	ID	Version	Filename	Modified	Count	Number	Size
4 bytes	4 bytes	4 bytes	64 bytes	4 bytes	4 bytes	4 bytes	4 bytes

FIG. 11

UDP Header 628

Source Port	Dest. Port	UDP Length	UDP Checksum
2 bytes	2 bytes	2 bytes	2 bytes

FIG. 12

IP Packet Header (Version 4) 632

Version	Header Length	Type of Service	Total Length	Identification	Flags
4 bits	4 bits	1 byte	2 bytes	2 bytes	3 bits

Fragment Offset	Time to Live	Protocol	Header Checksum	Source IP Address
13 bits	1 byte	1 byte	2 bytes	4 bytes

Destination IP Address	Options
4 bytes	

FIG. 13

MPT Start Packet 730

Flags	SOF	EOF	sub-SCID Address	Frame Type	Data
6 bits	1 bit	1 bit	6 bytes	2 bytes	118 bytes

FIG.14A

MPT Middle Packet(s) 740

Flags	SOF	EOF	Data
6 bits	1 bit	1 bit	126 bytes

FIG.14B

MPT End Packet 750

Flags	SOF	EOF	Data	CRC
6 bits	1 bit	1 bit	122 bytes	4 bytes

FIG.14C

MPT Only Packet 760

Flags	SOF	EOF	sub-SCID Address	Frame Type	Data	CRC
6 bits	1 bit	1 bit	6 bytes	2 bytes	114 bytes	4 bytes

FIG.14D

BARP Header

Version	Change Number	Record Count	Reserved
1 byte	1 byte	2 bytes	4 bytes

FIG.15A

BARP Address Record

IP Address	Transponders	SCID	Channel	Service Type	Reserved
4 bytes	4 bytes	2 bytes	2 bytes	1 byte	3 bytes

FIG.15B

Example Ticker SDP+ Record
v=0
o=DTV 0001 17 DSS IP4
s=Announcement Dump
c=DSS IP4 233.17.43.6/1
t=0 0
m=data 3287 UDP STREAM
a=key:1
a=run:consoleticker
a=keywds:tsetup

FIG.16A

Example File Download SDP+ Record
v=0
o=DTV 0008 17 DSS IP4
s=Data Catalog
c=DSS IP4 233.17.43.3/1
t=3079382400 3155745600
r=10m 10m 0
m=data 3335 UDP BFDP
a=key:8
a=fsz:980000
a=mandatory
a=run:cataloginstall.exe

FIG.16B

Example Webcast SDP+ Record
v=0
o=DTV 900 17 DSS IP4
s=CNN
i=Research financial markets worldwide, get stack quotes, and calculate your mortgage payments - all on-line. Read the "hot stories" of the week in the financial world. Complete listing of CNN's Financial Network television broadcasts.
u=http://www.cnn.com/index.htm
c=DSS IP4 233.17.43.7/1
t=0 0
m=data 3334 UDP WEBCAST
a=cat:News
a=key:900
a=fsz:16000000
a=display:type=1, priority=8
a=img:cnn.gif

FIG.16C

Example data enriched video SDP+ record
v=0
o=DTV 0201 17 DSS IP4
s=CNBC
c=DSS IP4 233.26.24.24/1
t=0 0
m=data 6500 UDP INTERCAST
a=key:201
a=channel:775

FIG.16D

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 071 296 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
24.01.2001 Bulletin 2001/04

(51) Int Cl.7: **H04Q 7/22**

(21) Application number: **99401864.6**

(22) Date of filing: **22.07.1999**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(71) Applicant: **ALCATEL**
75008 Paris (FR)

(72) Inventors:
- **Leroy, Suresh André Jean-Marie**
  2970 Schilde (BE)
- **Ramalho, Maria Fernanda**
  1170 Brussels (BE)
- **Sales, Bernard**
  1190 Brussels (BE)
- **Aerts, Helena Tine**
  2000 Antwerp (BE)

(74) Representative: **Plas, Axel**
Alcatel Bell N.V.,
Francis Wellesplein 1
2018 Antwerpen (BE)

(54) Method to multi-cast data packets to mobile stations, and related gateway, service and routing nodes

(57) To transfer public data packets (PU-DP) from an originating terminal (TE) to a plurality of mobile stations (MS1, MS2, MS3, MS4, MS6) over a public data packet network (INTERNET) and a mobile data packet network (GPRS-SYSTEM), the public data packets (PU-DP) are multi-casted through the public data packet network (INTERNET) by means of a multi-cast address (PU-MCA) in an overhead section (PU-H) of the public data packets (PU-DP). In addition, the public data packets (PU-DP) are multi-casted through at least part of the mobile data packet network (GPRS-SYSTEM) by means of a private multi-cast address (PR-MCA) in an overhead section (PR-H) of private data packets (PR-DP) that tunnel the public data packets (PU-DP) through the mobile data packet network (GPRS-SYSTEM).

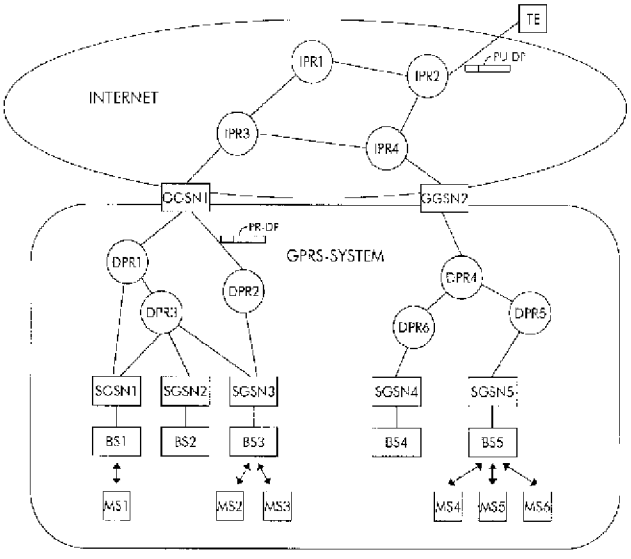


Fig. 1

EP 1 071 296 A1

Description

[0001] The present invention relates to a method to transfer data packets over a public data packet network and a mobile data packet network to a plurality of mobile stations as defined in the non-characteristic part of claim 1, a gateway node for interfacing between the public data packet network and the mobile data packet network as defined in the non-characteristic part of claim 2, a service node for serving mobile stations in the mobile data packet network as defined in the non-characteristic part of claim 6, and a routing node for routing data packets in between gateway nodes and service nodes of the mobile data packet network as defined in the non-characteristic part of claim 9.

[0002] Such a method for transferring data packets through a mobile data packet network, as well as a gateway node, service node and routing node of the mobile data packet network are already known in the art, e.g. from *the standard specification "Digital Cellular Telecommunications System (Phase 2+); General Packet Radio Service (GPRS); Service Description; Stage 2", published by ETSI (European Telecommunications Standards Institute) under the reference TS/SMG-030360Q. This standard specification is also named "GSM 03.60 Version 6.0.0" but will be referred to by "GPRS Specification" in the remainder of this patent application.* The GPRS Specification describes a data packet service for a mobile communication network that makes use of the GSM (Global System for Mobile Communications) air interface for the communication between base stations and mobile stations. For the communication up to the base stations, the GPRS Specification introduces two new network nodes: a Gateway GPRS Support Node (GGSN) provides inter-working between an external or public packet switching network and the mobile or private packet switching network, whereas a Serving GPRS Support Node (SGSN) keeps track of the individual mobile stations within a certain service area, and performs security functions, access control and mobility functions, e.g. change of SGSN by a mobile station. The architecture of a GPRS (General Packet Radio Service) system built up of Gateway GPRS Support Nodes, Serving GPRS Support Nodes, Base Stations and Mobile Stations is illustrated by Figure 2 and Figure 3 respectively on page 18 and 19 of the above cited GPRS Specification. Figure 4 on page 21 gives an overview of the protocol stack used for transferring data packets through the GPRS system. To route data packets received from an external data packet network like the internet to a mobile station in the known GPRS system, a so called point-to-point tunnel is set up from the Gateway GPRS Support Node (GGSN) that receives the data packets from the external data packet network to the Serving GPRS Support Node (SGSN) in whose service area the mobile station is residing. This means that the external data packets are encapsulated in internal data packets in the Gateway GPRS Support Node, that these internal data packets are routed to the Serving GPRS Support Node accordance with an internal routing protocol, and that the external data packets are de-capsulated from the internal data packets in the Serving GPRS Support Node to be forwarded to the Base Station that will send the data packets to the mobile station over the air interface.

[0003] If in the known GPRS system the same data packets have to be transferred to more than one mobile station residing in the same service area, for instance because these mobile stations are members of the same multicast group in the external network, these data packets will independently be forwarded from the Gateway GPRS Support Node (GGSN) to the different mobile stations via separate point-to-point tunnels. In such situations, network resources are inefficiently used in the known mobile data packet network because duplicated data packets are transferred over the common part of the routes to the different mobile terminals.

[0004] An object of the present invention is to provide a method for transferring data packets through a mobile data packet network, as well as a gateway node, a service node and a routing node similar to the above known ones, but which use network resources, i.e. bandwidth capacity, more efficiently in case the same data packets have to be routed to a plurality of mobile terminals.

[0005] According to the invention, this object is achieved by the method to transfer data packets over a public data packet network and a mobile data packet network to a plurality of mobile stations as defined in claim 1, the gateway node for interfacing between the public data packet network and the mobile data packet network as defined in claim 2, the service node for serving mobile stations in the mobile data packet network as defined in claim 6, and the routing node for routing data packets in between gateway nodes and service nodes of the mobile data packet network as defined in claim 9.

[0006] Indeed, by multi-casting the internal data packets (named private data packets in the remainder of this patent application because they are routed within the mobile data packet network that is usually owned by a private operator) that tunnel external data packets (named public data packets in the remainder of this patent application because they are routed through a public data packet network such as the internet) that belong to an external multi-cast connection, it is avoided that the same public data packets are duplicated and encapsulated in different private data packets that are transferred over at least partially common routes in the mobile data packet network. Multi-casting internal data packets is realised via internal multi-cast addresses associated with external multi-cast groups where a mobile station can subscribe to. When a gateway node receives public data packets for a multi-cast connection, it will send these data packets on the private multi-cast tree which contains service nodes that contain members of the external multi-cast group in their service area. The service nodes further send the data packets to the mo-

bile stations that are member of the multi-cast group via point-to-point connections. In this way, the network resources for transfer of data between the gateway nodes and the service nodes are used more efficiently and the capacity of the mobile data packet network is enlarged significantly in particular if the share of multi-cast traffic in the aggregate data traffic is significant.

[0007] It is to be noticed that the term 'comprising', used in the claims, should not be interpreted as being limitative to the means listed thereafter. Thus, the scope of the expression 'a device comprising means A and B' should not be limited to devices consisting only of components A and B. It means that with respect to the present invention, the only relevant components of the device are A and B.

[0008] Similarly, it is to be noticed that the term 'coupled', also used in the claims, should not be interpreted as being limitative to direct connections only. Thus, the scope of the expression 'a device A coupled to a device B' should not be limited to devices or systems wherein an output of device A is directly connected to an input of device B. It means that there exists a path between an output of A and an input of B which may be a path including other devices or means.

[0009] An additional feature of the gateway node according to the present invention is defined by claim 3.

[0010] This, a mobile station can become member of a public multi-cast group by transmitting a public join message towards a gateway node. The gateway node can interpret this public join message and inform the service node in whose service area the mobile station is residing, that the mobile station becomes member of the public multi-cast group via a private join message. The private join message is addressed to the service node and contains the public join message received by the gateway node. It is necessary to first transfer the public join message to the gateway node and to feed back the public join message encapsulated in a private message to the service node because the service node cannot interpret the public join message transmitted by the mobile station towards the gateway node.

[0011] An alternative way of joining the public multi-cast group requires that the mobile station sends a GPRS specific join message that can be interpreted by both the service node and the gateway node. This alternative does not require feedback of join messages from the gateway node to the service node but involves modification of the GPRS standard specification because the format of such a GPRS specific join message has to be standardised.

[0012] Another feature of the gateway node according to the present invention is defined in claim 4.

[0013] In this way, by assigning to the private multi-cast group that is associated with a public multi-cast group a private multi-cast address that is equal to the public multi-cast address, complexity of the address association means in the gateway node is minimised. No table linking the private multi-cast addresses with the public multi-cast addresses has to be maintained in gateway nodes and service nodes.

[0014] Compared to claim 4, an alternative implementation of the gateway node according to the present invention is defined by claim 5.

[0015] In this way, the address association means in the gateway node needs to keep track of a table wherein public multi-cast addresses and associated private multi-cast addresses are memorised which makes the address association means more complex but creates a greater flexibility in assignment and use of private multi-cast addresses.

[0016] An additional feature of the service node according to the present invention is defined in claim 7.

[0017] Thus, the service node is able to maintain a list of mobile stations which are member of a public multi-cast group. The service node updates the table wherein public multi-cast addresses, private multi-cast addresses and mobile stations are linked upon receipt of join/leave messages sent to it by a gateway node.

[0018] As an alternative to claim 7, claim 8 specific that the table wherein public multi-cast addresses, private multi-cast addresses and mobile stations are linked may be updated upon receipt of GPRS specific join/leave messages from mobile stations that want to join/leave a public multi-cast group. Such a GPRS specific join/leave message can be interpreted by the service node if its format is standardised.

[0019] The above mentioned and other objects and features of the invention will become more apparent and the invention itself will be best understood by referring to the following description of an embodiment taken in conjunction with the accompanying drawings wherein:

Fig. 1 represents an architectural scheme of a system including gateway nodes GGSN1 and GGSN2 according to the present invention, service nodes SGSN1, SGSN2, SGSN3, SGSN4 and SGSN5 according to the present invention, and routing nodes DPR1, DPR2, DPR3, DPR4, DPR5 and DPR6 according to the present invention;

Fig. 2 illustrates the structure of a private data packet PR-DP multi-casted according to the present invention;

Fig. 3 represents a functional block scheme of an embodiment of the gateway node GGSN1 according to the present invention; and

Fig. 4 represents a functional block scheme of an embodiment of the service node SGSN3 according to the present invention.

[0020] Fig. 1 shows the internet INTERNET and a General Packet Radio Service system GPRS-SYSTEM. The internet INTERNET contains a plurality of IP (Internet Protocol) routers IPR1, IPR2, IPR3 and IPR4 interconnected via links and one terminal TE of the internet INTERNET is also drawn. The General Packet Radio Service system GPRS-SYSTEM contains two Gateway

GPRS Supporting nodes GGSN1 and GGSN2, a number of data packet routers DPR1, DPR2, DPR3, DPR4, DPR5 and DPR6, five Service GPRS Supporting nodes SGSN1, SGSN2, SGSN3, SGSN4 and SGSN5, and five base stations BS1, BS2, BS3, BS4 and BS5. Also six mobile stations or terminals of the GPRS-SYSTEM are drawn in Fig. 1: MS1, MS2, MS3, MS4, MS5 and MS6.

[0021] In the internet INTERNET, the first IP router IPR1 is connected to both the second IP router IPR2 and to the third IP router IPR3. The second IP router IPR2 is connected to the fourth IP router IPR4, the third IP router IPR3 is connected respectively to the first gateway node GGSN1 and to the fourth IP router IPR4, and the just mentioned fourth IP router IPR4 is connected to the second gateway node GGSN2. The terminal TE is interconnected with the second IP router IPR2. In the GPRS-SYSTEM, the first gateway node GGSN 1 is connected to both the first data packet router DPR1 and the second data packet router DPR2. The first data packet router DPR1 additionally is interconnected with the third data packet router DPR3 and the first service node SGSN1, whereas the second data packet router DPR2 is only interconnected with the third service node SGSN3. The third data packet router DPR3 is connected to the first service node SGSN1, the second service node SGSN2 and the third service node SGSN3. These first, second and third service nodes SGSN1, SGSN2 and SGSN3 are respectively connected to the first, second and third base stations BS1, BS2 and BS3. The second gateway node GGSN2 is connected to the fourth data packet router DPR4. This fourth data packet router DPR4 further is connected to the fifth data packet router DPR5 and to the sixth data packet router DPR6. The fifth data packet router DPR5 and the fifth service node SGSN5 are interconnected, and also the sixth data packet router DPR6 and the fourth service node SGSN4 are interconnected. The just mentioned fourth service node SGSN4 is connected to the fourth base station BS4 and the earlier mentioned fifth service node SGSN5 is connected to the fifth base station BS5. The first mobile station MS1 is located within the service area of the first service node SGSN1, the second mobile station MS2 as well as the third mobile station MS3 are located within the service area of the third service node SGSN3. Mobile stations MS4, MS5 and MS6 are all located in the service area of the fifth service node SGSN5.

[0022] In the internet INTERNET data are communicated in accordance with the internet protocol (IP). Data in other words are encapsulated in IP packets PU-DP. Such an IP packet PU-DP is shown in Fig. 2 and contains an overhead section or IP header PU-H and a payload section wherein user data can be embedded. One field of the IP header PU-H carries the address of the destination of the IP data packet PU-DP. In case the IP data packet PU-DP is destined to all members of a multicast group, the sender of the IP data packet PU-DP will embed an internet multi-cast address PU-MCA in the destination address field of that IP data packet PU-DP. The internet terminal TE in Fig. 1 for example is supposed to have sent an IP data packet PU-DP to such a multi-cast group. The IP routers IPR1, IPR2, IPR3 and IPR4 have the task to route IP data packets from their origin to their destination(s). The IP routers IPR1, IPR2, IPR3 and IPR4 thereto look at the contents of the destination address field of the IP data packets they receive and can route the IP data packets either by consulting routing tables or via explicit routing techniques. In case an IP router, IPR1, IPR2, IPR3 or IPR4 receives an IP data packet PU-DP whose destination address field contains an internet multi-cast address PU-MCA, the IP router will multi-cast the data packet PU-DP: the data packet PU-DP is then forwarded to the IP routers that joined the multi-cast tree whereover such IP data packets PU-DP are routed towards all members of the multicast group.

[0023] In the GPRS-SYSTEM data packets are routed towards mobile stations in accordance with the GPRS standard specification, whereto reference is made in the introductory part of this patent application. The gateway nodes GGSN1 and GGSN2 provide interworking with the internet INTERNET, and encapsulate an IP data packet PU-DP received from the internet INTERNET in a private data packet PR-DP that can be routed through the GPRS-SYSTEM towards the destination mobile stations. This operation is known as tunneling. Such a private data packet PR-DP wherein the IP data packet PU-DP is encapsulated, is shown in Fig. 2. This private data packet PR-DP also contains an overhead section PR-H and a payload section wherein the IP data packet PU-DP is embedded. In accordance with the GPRS standard specification, the private data packet PR-DP is a private IP (Internet Protocol) packet and consequently the overhead section PR-H thereof is an IP (Internet Protocol) header wherein also one field is reserved for the destination address of the private data packet PR-DP. As will be explained further, the gateway node GGSN1 that encapsulates the IP data packet PU-DP in the private data packet PR-DP fills the destination address field of the private data packet header PR-H with a private multi-cast address PR-MCA when the destination address field of the IP data packet PU-DP contains an internet multi-cast address PU-MCA.

[0024] The data packet routers DPR1, DPR2, DPR3, DPR4, DPR5 and DPR6 include the functionality to route a private data packet PR-DP to its destination or destinations and, similarly to the IP routers IPR1, IPR2, IPR3 and IPR4 in the internet INTERNET, thereto look at the contents of the destination address field of the private data packets PR-DP and consult routing tables or perform explicit routing techniques. The service nodes SGSN1, SGSN2, SGSN3, SGSN4 and SGSN5 keep track of the locations of the mobile stations and perform mobility security functions and access control compliant with the GPRS standard specification. Via the base stations BS1, BS2, BS3, BS4 and BS5, the service

nodes SGSN1, SGSN2, SGSN3, SGSN4 and SGSN5 are able to set up radio connections to the mobile stations MS1, MS2, MS3, MS4, MS5 and MS6 so that the data packets can be delivered to the mobile stations MS1, MS2, MS3, MS4, MS5 and MS6.

[0025] In the following paragraphs, it will be supposed that the internet terminal TE is the origin of internet data packets PU-DP destined to the members of a multi-cast group with internet multi-cast address PU-MCA. The mobile stations MS1, MS2, MS3, MS4 and MS6 want to receive such data packets and thereto request to become member of this internet multi-cast group. The registration of these mobile stations MS1, MS2, MS3, MS4 and MS6 as members of the multi-cast group, as well as the way wherein the internet data packets PU-DP destined to the members of this multi-cast group are routed towards the mobile stations MS1, MS2, MS3, MS4 and MS6 in accordance with the principles of the present invention will be explained in the next paragraphs. Reference will be made to Fig. 3 and Fig. 4 in these paragraphs to address the required functionality respectively in the gateway nodes GGSN1 and GGSN2 and the service nodes SGSN1, SGSN2, SGSN3, SGSN4 and SGSN5 to be able to fulfil the principles of the present invention.

[0026] Gateway node GGSN1 of Fig. 1 is drawn in more detail in Fig. 3 and includes an internet multi-cast address recognition device PU-RECOGNITION, a multi-cast address association device PU-PR-ASSOCIATION, a private data packet generator PR-GENERATION, a private data packet transmitter PR-TX, a multi-cast address table PU-PR-TABLE, a routing table ROUTING-TABLE, a public join/leave message receiver PU-JN/LV RX, and a private join/leave message generator PR-JN/LV GENERATOR.

[0027] The internet multi-cast address recognition device PU-RECOGNITION, the multi-cast address association device PU-PR-ASSOCIATION, the private data packet generator PR-GENERATION, and the private data packet transmitter PR-TX are cascade coupled between a port of the gateway node GGSN1 whereto the third IP router IPR3 is connected in Fig. 1 and a port of the gateway node GGSN1 whereto the data packet routers DPR1 and DPR2 of the GPRS-SYSTEM in Fig. 1 are coupled. The multi-cast address table PU-PR-TABLE interfaces with the multi-cast address association device PU-PR-ASSOCIATON, and the routing table ROUTING-TABLE interfaces with the private data packet transmitter PR-TX. The public join/leave message receiver PU-JN/LV RX is connected to the port of gateway node GGSN1 whereto data packet routers DPR1 and DPR2 are coupled. The public join/leave message receiver PU-JN/LV RX further is coupled to the private data packet transmitter PR-TX via the private join/leave message generator PR-JN/LV GENERATOR, and also interfaces with the routing table ROUTING-TABLE.

[0028] The service node SGSN3 of Fig. 1 is drawn in more detail in Fig. 4 and includes a private multi-cast address recognition device PR-RECOGNITION, a private data packet copier and transmitter COPY/SEND, a multi-cast group registration device MS-REGISTRATION, and a private join/leave message receiver PR-JN/LV RX.

[0029] The private multi-cast address recognition device PR-RECOGNITION and the private data packet copier and transmitter COPY/SEND are cascade coupled between a port of the service node SGSN3 that is coupled to the data packet routers DPR2 and DPR3 in Fig. 1, and a port of the service node SGSN3 whereto the base station BS3 is coupled. To the port coupled to data packet routers DPR2 and DPR3 also the private join/leave message receiver PR-JN/LV RX is connected and this private join/leave message receiver PR-JN/LV RX has an output terminal coupled to an input terminal the multi-cast group registration device MS-REGISTRATION. The multi-cast group registration device MS-REGISTRATION interfaces with the private data packet copier and transmitter COPY/SEND.

[0030] If the second mobile station MS2 wants to become member of the multi-cast group with internet multi-cast address PU-MCA, it will send a public join message to the service node SGSN3 in whose service area the mobile station MS2 is residing. The service node SGSN3 cannot interpret this public join message and transparently transfers the join message via the data packet routers to gateway node GGSN1. In the gateway node GGSN1, the public join/leave message receiver PU-JN/LV RX receives the public join message and interprets this message. The private multi-cast tree in GPRS-SYSTEM is updated so that the internet data packets PU-DP addressed to the internet multi-cast address PU-MCA will be routed to the mobile station MS2. In addition, the public join message is encapsulated in a private join message by the private join/leave message generator PR-JN/LV GENERATOR and this private join message is sent to the service node SGSN3 in whose service area mobile station MS2 is residing. In this way, the service node SGSN3 is made aware that the mobile station MS2 becomes member of the multi-cast group with the internet multi-cast address PU-MCA and private multi-cast address PR-MCA. Indeed, this multi-cast group is addressed within the GPRS-SYSTEM with a private multi-cast address PR-MCA that is linked to the public multi-cast address PU-MCA via a table PU-PR-TABLE in the gateway node GGSN1 and via the multi-cast group registration device MS-REGISTRATION in the service node SGSN3. The just mentioned multi-cast group registration device MS-REGISTRATION upon instruction of the private join/leave message receiver PR-JN/LV RX memorises that mobile station MS2 becomes member of the multi-cast group with public multi-cast address PU-MCA and private multi-cast address PR-MCA. It is the task of the gateway node GGSN1 to mention to the IP router IPR3 that it wants to join the internet multi-cast group with internet multi-cast address PU-MCA. Similarly to mobile station MS2, mo-

bile station MS3 will join the public multi-cast group with internet multi-cast address PU-MCA. A public join message is transmitted towards gateway node GGSN1 and returned as a private join message to the service node SGSN3 in whose area the mobile station MS3 is located. In the multi-cast group registration device MS-REGISTRATION it is memorised that mobile station MS3 also wants to receive the private data packets destined to the multi-cast group with public multi-cast address PU-MCA and private multi-cast address PR-MCA. Also mobile stations MS1, MS4 and MS6 become members of the multi-cast group which is addressed by the internet multi-cast address PU-MCA in the INTERNET and which is addressed by the private multi-cast address PR-MCA in the GPRS-SYSTEM. Mobile station MS1 for example is registered as member of this multi-cast group in the service node SGSN1, In a similar way, service node SGSN5 registers that the mobile stations MS4 and MS6 have joined this multi-cast group.

[0031] Summarising, a registration mechanism is provided in the GPRS-SYSTEM whereby the service nodes SGSN 1, SGSN2, SGSN3, SGSN4 and SGSN5 register which mobile terminals MS1, MS2, MS3, MS4 and MS6 joined a public multi-cast group via a join message that is sent to a gateway node and returned thereby as a private join message. In case a mobile station moves to another service area, the registered information must be updated. This update may form part of the inter SGSN routing area update procedure in a cellular mobile system. In case a mobile station wants to be deleted as member of a public multi-cast group, it will send a leave message which is treated in a similar way as the join messages. The service node thereupon de-registers the mobile station as member of the multi-cast group.

[0032] If an internet server or a terminal TE transmits internet data packets PU-DP addressed to members of the internet multi-cast group with internet multi-cast address PU-MCA, these packets will be routed to the gateway nodes GGSN1 and GGSN2 because these gateway nodes joined the multi-cast tree associated with that internet multi-cast group as explained above. The internet multi-cast address recognition device PU-RECOGNITION in gateway node GGSN1 detects that the received internet data packet PU-DP is addressed to the internet multi-cast group by recognising internet multi-cast address PU-MCA in the destination address field of the internet data packet PU-DP. The internet multi-cast recognition device PU-RECOGNITION instructs the multi-cast address association device PU-PR-ASSOCIATION to retrieve from the multi-cast address table PU-PR-TABLE the private multi-cast address PR-MCA that is associated with the internet multi-cast address PU-MCA. This private multi-cast address PR-MCA in an alternative embodiment of the invention without multi-cast address table PU-PR-TABLE may be equal to the public multi-cast address PU-MCA. The internet data packet PU-DP is encapsulated in a private data packet PR-DP by the private data packet generator PR-GENERATION and is forwarded by the private data packet transmitter PR-TX over the private multi-cast tree addressed via private multi-cast address PR-MCA. The private data packet transmitter PR-TX thereto consults the routing table ROUTING-TABLE. The internet data packet PU-DP, encapsulated in the private data packet PR-DP, consequently is multi-casted once to the service node SGSN3 and not transferred two times to service node SGSN3 because two mobile stations MS2 and MS3 in its service area want to receive this data packet PU-DP. In the service node SGSN3, the private multi-cast address recognition device PR-RECOGNITION recognises the private multi-cast address PR-MCA in the header PR-H of the private data packet PR-DP and thereupon instructs the data packet copier and transmitter COPY/SEND to send copies of the data packet PU-DP to all mobile stations, MS2 and MS3, that are member of the public multi-cast group addressed via the public multi-cast address PU-MCA. The private data packet copier and transmitter COPY/SEND thereto consults the memory of the multi-cast group registration device MS-REGISTRATION. In a similar way as described for mobile stations MS2 and MS3, the public data packet PU-DP will be routed to the mobile station MS1 and will be routed to the mobile stations MS4 and MS6. To transfer the data packet PU-DP to mobile stations MS4 and MS6, the data packet again will be multi-casted only once to service node SGSN5, which will duplicate the data packet PU-DP and send a copy to each one of the mobile stations MS4 and MS6.

[0033] Summarising, the private data packets PR-DP wherein public data packets PU-DP destined to an internet multi-cast group are encapsulated, are multi-casted in the GPRS-SYSTEM up to the level of the service nodes. This is made possible by associating private multi-cast groups with the internet multi-cast groups and by maintaining in the service nodes which mobile stations are member of the different public multi-cast groups. In this way, the required bandwidth for transfer of multi-cast traffic between the gateway nodes and the service nodes of the GPRS-SYSTEM is reduced significantly.

[0034] Although implementation of the invention has been described above for transfer of internet data packets over the internet and over a GPRS system interfacing with the internet, it is clear that the same principles can be applied to transfer for example IP or X.25 data packets over respectively an IP or X.25 network and a UMTS (Universal Mobile Telecommunications System) system, interfacing with the IP or X.25 network. In fact the invention can be applied in any system wherein private mobile data packets tunnel public data packets received from a public or external data packet network towards mobile stations, irrespective of the particular protocol that is used in the public data packet network and the mobile network.

[0035] It is also remarked that introduction of the present invention in a GPRS system is not complex because a GPRS system already uses the Internet Proto-

col to tunnel public data packets from the gateway nodes to the service nodes. Introduction of private multi-cast IP addresses, similar to the public multi-cast group IP addresses that are used in the internet makes the invention feasible. No adaptation of the protocol is required in the GPRS system to enable introduction of the present invention.

[0036] Furthermore it is noticed that the private multi-cast address and public multi-cast address associated with each other can be equal. The association of a private multi-cast address with a public multi-cast address then becomes very simple because no tables are required in the gateway nodes and service nodes. The flexibility in use of private addresses is increased if the private multi-cast address associated with a public multi-cast address is not equal thereto. The link between private and public multi-cast addresses then however has to be memorised in a centralised or distributed database.

[0037] While the principles of the invention have been described above in connection with specific apparatus, it is to be clearly understood that this description is made only by way of example and not as a limitation on the scope of the invention.

Claims

1. Method to transfer public data packets (PU-DP) from an originating terminal (TE) to at least a plurality of mobile stations (MS1, MS2, MS3, MS4, MS6) over a public data packet network (INTERNET) and a mobile data packet network (GPRS-SYSTEM) whereby said public data packets (PU-DP) are multi-casted through said public data packet network (INTERNET) by means of a multi-cast address (PU-MCA) in an overhead section (PU-H) of said public data packets (PU-DP),

   CHARACTERISED IN THAT said public data packets (PU-DP) are further multi-casted through at least part of said mobile data packet network (GPRS-SYSTEM) by means of a private multi-cast address (PR-MCA) in an overhead section (PR-H) of private data packets (PR-DP) that tunnel said public data packets (PU-DP) through at least said part of said mobile data packet network (GPRS-SYSTEM).

2. Gateway node (GGSN1) for interfacing between a public data packet network (INTERNET) and a mobile data packet network (GPRS-SYSTEM), said gateway node (GGSN1) comprising:

   a. public multi-cast address recognition means (PU-RECOGNITION) to recognise a public multi-cast address (PU-MCA) in an overhead section (PU-H) of public data packets (PU-DP) sent from an originating terminal (TE) to at least a plurality of mobile stations (MS1, MS2, MS3, MS4, MS6) over said public data packet network (INTERNET) and said mobile data packet network (GPRS-SYSTEM),

   CHARACTERISED IN THAT said gateway node (GGSN 1) further comprises:

   b. address association means (PU-PR-ASSOCIATION) to associate a private multi-cast address (PR-MCA) with said public multi-cast address (PU-MCA); and

   c. private data packet generation means (PR-GENERATION) to generate private data packets (PR-DP) for tunnelling said public data packets (PU-DP) through at least part of said mobile data packet network (GPRS-SYSTEM) towards said mobile stations (MS1, MS2, MS3, MS4, MS6), said private data packets (PR-DP) having said private multi-cast address (PR-MCA) in an overhead section thereof.

3. Gateway node (GGSN 1) according to claim 2,

   CHARACTERISED IN THAT said gateway node (GGSN 1) further comprises:

   d. public join/leave message receiving means (PU-JN/LV RX), adapted to receive a join/leave message from a mobile station (MS2) indicating that said mobile station (MS2) wants to join/leave a public multi-cast group; and

   e. private join/leave message generating means (PR-JN/LV GENERATION), coupled to said public join/leave message receiving means (PU-JN/LV RX) and adapted to generate a private data packet for tunnelling said join/leave message from said gateway node (GGSN1) to a service node (SGSN3) of said mobile data packet network (GPRS-SYSTEM) serving said mobile station (MS2).

4. Gateway node (GGSN1) according to claim 2 or claim 3,

   CHARACTERISED IN THAT said address association means (PU-PR-ASSOCIATION) is adapted to associate with said public multi-cast address (PU-MCA) a private multi-cast address (PR-MCA) that is equal to said public multi-cast address (PU-MCA).

5. Gateway node (GGSN1) according to claim 2 or claim 3,

   CHARACTERISED IN THAT said address association means (PU-PR-ASSOCIATION) is adapted to associate with said public multi-cast address (PU-MCA) a private multi-cast address (PR-MCA) linked to said public multi-cast address (PU-MCA) via a table (PU-PR-TABLE) comprised in said gateway node (GGSN 1).

6. Service node (SGSN3) for serving in a mobile data pocket network (GPRS-SYSTEM) data packet communication to mobile stations (MS2, MS3) within a certain service area,

CHARACTERISED IN THAT said service node (SGSN3) comprises:

a. private multi-cast address recognition means (PR-RECOGNITION) to recognise a private multi-cast address (PR-MCA) in an overhead section (PR-H) of private data packets (PR-DP) that tunnel through at least part of said mobile data packet network (GPRS-SYSTEM) public data packets (PU-DP) sent from an originating terminal (TE) over a public data packet network (INTERNET) and said mobile data packet network (GPRS-SYSTEM) to at least a plurality of mobile stations (MS2, MS3) within said service area; and

b. means (COPY/SEND) to generate copies of said public data packets (PU-DP) and to send a copy to each one of said mobile stations (MS2, MS3).

7. Service node (SGSN3) according to claim 6,

CHARACTERISED IN THAT said service node (SGSN3) further comprises:

c. private join/leave message receiving means (PR-JN/LV RX) adapted to receive a private join/leave message indicating that a mobile station (MS2) wants to join/leave a public multi-cast group; and

d. registration means (MS-REGISTRATION), coupled to said private join/leave message receiving means (PR-JN/LV RX), and adapted to register inclusion and deletion of a mobile station (MS2).

8. Service node (SGSN3) according to claim 6,

CHARACTERISED IN THAT said service node (SGSN3) further comprises:

e. GPRS join/leave message receiving means to receive a GPRS message indicating that a mobile station (MS2) wants to join/leave a public multi-cast group; and

f. registration means (MS-REGISTRATION) coupled to said GPRS join/leave message receiving means and adapted to register inclusion and deletion of said mobile station (MS2) to or from said public multi-cast group.

9. Routing node (DPR1, DPR2, DPR3, DPR4, DPR5, DPR6) for routing private data packets (PR-DP) from a gateway node (GGSN1) to at least one service node (SGSN 1, SGSN3) of a mobile data packet network (GPRS-SYSTEM), said private data packets (PR-DP) being adapted to tunnel public data packets (PU-DP) sent from an originating terminal (TE) over a public data packet network (INTERNET) and said mobile data packet network (GPRS-SYSTEM) to at least a plurality of mobile stations (MS1, MS2, MS3, MS4, MS6),

CHARACTERISED IN THAT said routing node (DPR1, DPR2, DPR3, DPR4, DPR5, DPR6) comprises means to multi-cast said private data packets (PR-DP) by means of a private multi-cast address (PR-MCA) in an overhead section (PR-H) of said private data packets (PR-DP).

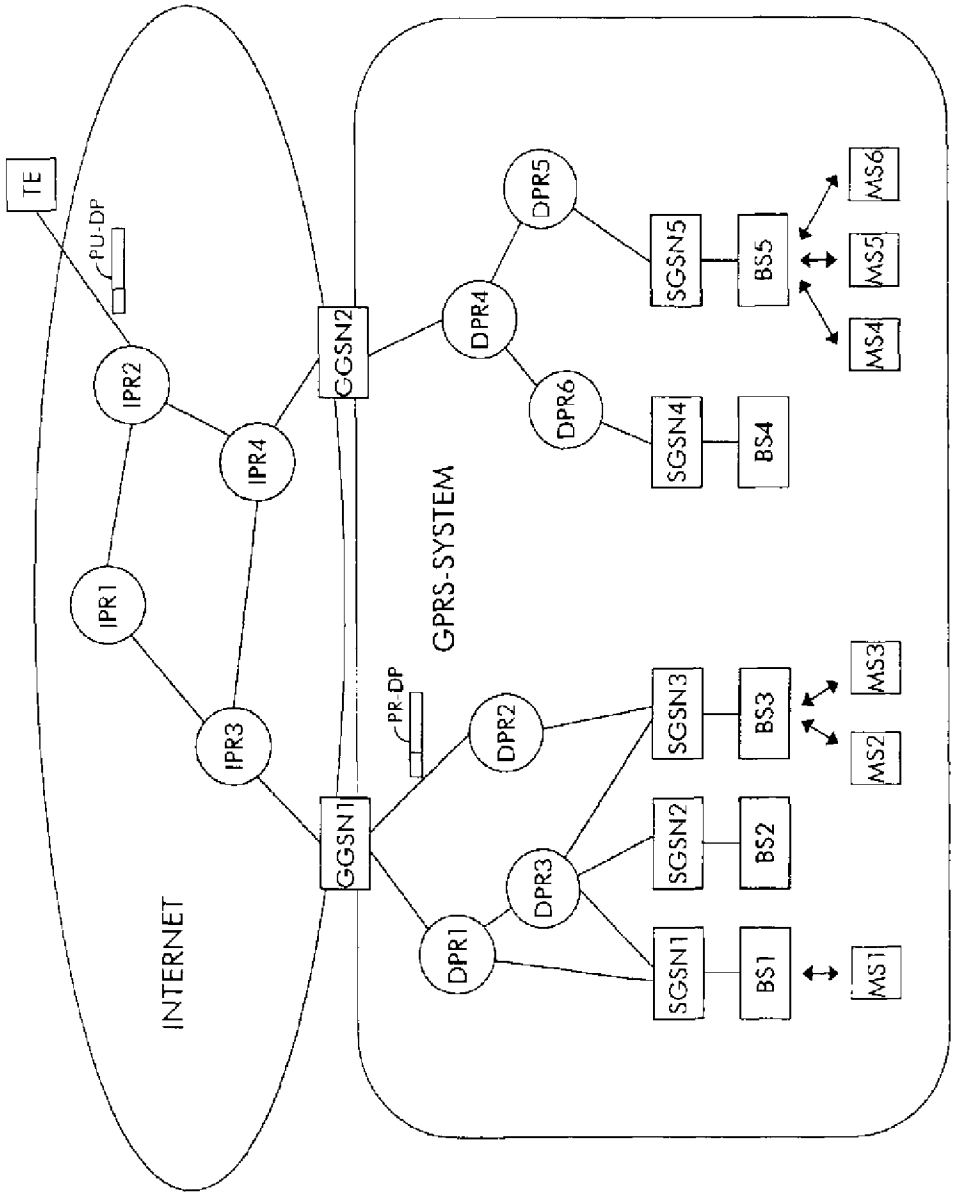

TE
PU-DP
IPR2
IPR4
IPR1
IPR3
INTERNET
GGSN2
GGSN1
PR-DP
GPRS-SYSTEM
DPR4
DPR5
DPR6
DPR2
DPR1
DPR3
SGSN5
SGSN4
SGSN3
SGSN2
SGSN1
BS5
BS4
BS3
BS2
BS1
MS6
MS5
MS4
MS3
MS2
MS1

Fig. 1

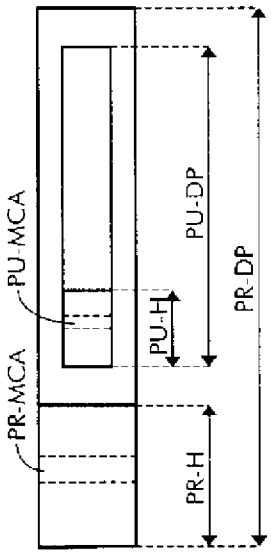

PU-MCA
PR-MCA
PU-H
PU-DP
PR-DP
PR-H

Fig. 2

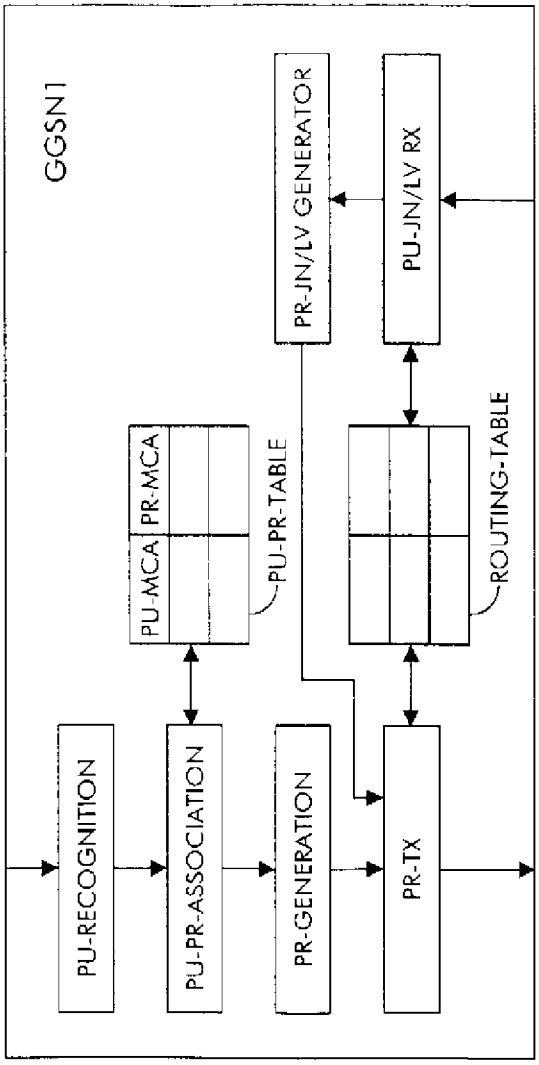

GGSN1
PU-RECOGNITION
PU-PR-ASSOCIATION
PR-GENERATION
PR-TX
PU-MCA
PR-MCA
PU-PR-TABLE
PR-JN/LV GENERATOR
PU-JN/LV RX
ROUTING-TABLE

Fig. 3

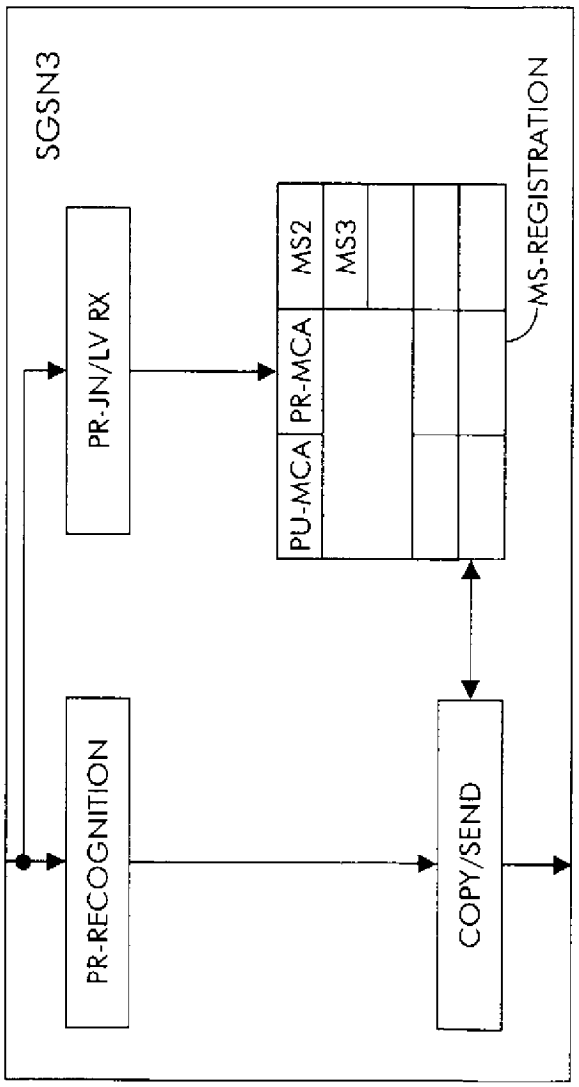

SGSN3
PR-JN/LV RX
PR-RECOGNITION
COPY/SEND
PU-MCA
PR-MCA
MS2
MS3
MS-REGISTRATION

Fig. 4

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 99 40 1864

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	WO 98 25422 A (NOKIA TELECOMMUNICATIONS OY ;HAUMONT SERGE (FI)) 11 June 1998 (1998-06-11) * page 1, line 3 - line 6 * * page 2, line 1 - line 13 * * page 3, line 12 - page 4, line 4 * * page 6, line 21 - line 36 * * page 11, line 3 - line 12 *	1,6-9	H04Q7/22
X	WO 97 21313 A (NORTHERN TELECOM LTD ;SAYERS IAN (GB); RICHARDSON KENNETH (GB)) 12 June 1997 (1997-06-12) * page 2, line 5 - line 20 * * page 5, line 4 - line 19 * * page 6, line 16 - line 35 *	1,2,6,9	
A	BRASCHE G: "EVALUATION OF A MAC PROTOCOL PROPOSED FOR A GENERAL PACKET RADIO SERVICE IN GSM" IEEE INTERNATIONAL SYMPOSIUM ON PERSONAL, INDOOR AND MOBILE RADIO COMMUNICATIONS, vol. 2, 1 May 1996 (1996-05-01), page 668-672 XP000198338 * page 669, left-hand column, line 20 - line 36 * * page 669, right-hand column, line 18 - line 28 *		TECHNICAL FIELDS SEARCHED (Int.Cl.7) H04Q H04L

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
BERLIN	9 December 1999	Rothlübbers, C

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 99 40 1864

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

09-12-1999

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9825422 A	11-06-1998	FI 964818 A	03-06-1998
		AU 5123398 A	29-06-1998
		EP 0947114 A	06-10-1999
WO 9721313 A	12-06-1997	GB 2307827 A	04-06-1997
		GB 2307828 A	04-06-1997

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 075 118 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
07.02.2001 Bulletin 2001/06

(51) Int Cl.7: **H04L 12/56**, H04L 29/12, H04L 12/18

(21) Application number: **00650087.0**

(22) Date of filing: **26.07.2000**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **30.07.1999 US 364339**

(71) Applicant: **Nortel Networks Limited**
Montreal, Quebec H2Y 3Y4 (CA)

(72) Inventors:
- **Basil, Nipun**
  Mass. 01821 (US)
- **Srikanth, Ayidudy**
  Reading, Mass. 01867 (US)
- **Meehan, Tom**
  Billerica, Mass. 01821 (US)

(74) Representative: **Coyle, Philip Aidan et al**
F. R. KELLY & CO.
27 Clyde Road
Ballsbridge
Dublin 4 (IE)

(54) Determining an end point of a GRE tunnel

(57) An end point address of a generic routing encapsulation (GRE) tunnel is obtained by forwarding a data packet through the GRE tunnel to devices at a multicast address. The data packet includes a logical address of a GRE tunnel end point device. A reply to the data packet is received from a remote GRE tunnel end point device. The reply includes a physical address of the remote GRE tunnel end point device.

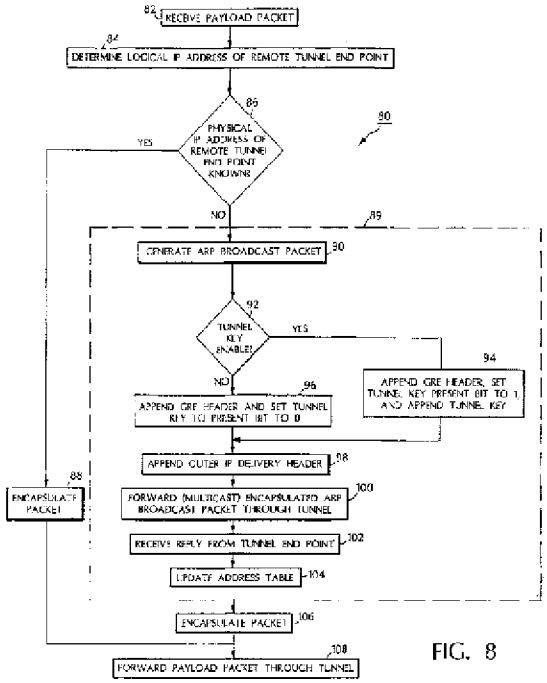


FIG. 8

EP 1 075 118 A2

Description

Background of the Invention

[0001] This invention relates to determining an end point of a generic routing encapsulation ("GRE") tunnel.

[0002] GRE is a protocol that enables the encapsulation of an arbitrary network layer protocol (the payload protocol) by another arbitrary network layer protocol (the delivery protocol). GRE tunnels are virtual tunnels that are created on an intermediary network and that are used to transmit GRE-encapsulated data packets from a first network to a second network. GRE tunnels are often used to create a virtual private network. ("VPN") by connecting two remote local area networks ("LAN") via the Internet.

[0003] At one end of a GRE tunnel, a router receives a payload packet from the first network, and encapsulates the payload packet so that it conforms to the delivery protocol of the intermediary network. The payload packet may be encapsulated in another packet or an Ethernet frame, for example. The encapsulated packet is transmitted through the intermediary network to the other end of the GRE tunnel. At that end, a router de-encapsulates the packet, and transmits the payload packet to the second network.

[0004] Heretofore, GRE tunnels were "static", meaning that the tunnel end points had to be configured, and updated, manually. For example, an address of a router at one tunnel end point may change, thereby making it necessary to provide the new address to other routers that use the tunnel end points. In a static GRE tunnel, a network administrator, using software such as Bay Command Console ("BCC") or Site Manager, enters this new information into each end point router manually. Manual reconfiguration is time-consuming and inefficient.

Summary of the Invention

[0005] In one aspect, the invention determines an end point of a GRE tunnel (e.g., an address of an end point device) by receiving a data packet at the device, identifying the data packet as a GRE packet, and determining an address of the end point of the GRE tunnel using the data packet. The address of the end point is stored in a table on the device. By determining an end point address using a GRE packet, the invention is able to provide routing updates automatically.

[0006] This aspect may include one or more of the following features and/or functions. Identifying comprises searching a header of the data packet for a value indicative of a GRE packet. The address ofthe end point comprises a logical address of the end point. The device is a router, and the data packet is a routing update packet.

[0007] Another aspect of the invention is directed to obtaining an end point address of a GRE tunnel dynamically. In this aspect, a data packet is forwarded through the GRE tunnel to a remote GRE tunnel end point device. In response, a reply is received from the remote GRE tunnel end point device, which includes a physical address of the remote GRE tunnel end point device.

[0008] This aspect provides a way for one device to obtain a physical address of a device at a remote tunnel end point. Thus, if end points have been added to, or removed from, the GRE tunnel, the invention can determine this dynamically and route packets accordingly.

[0009] The foregoing aspect may include one or more of the following features and/or functions.

[0010] The aspect of the invention may be performed by a local GRE tunnel end point device, and a table on the local GRE tunnel end point device may be updated to include the physical address of the remote GRE tunnel end point device. The reply includes a unicast address of the remote GRE tunnel end point device. The data packet comprises an address resolution protocol packet (ARP), and the ARP packet includes a logical address of the remote GRE tunnel end point device. The reply comprises a GRE-encapsulated data packet with the physical address of the remote GRE tunnel end point device as a payload.

[0011] This summary has been provided so that the nature of the invention can be understood quickly. A detailed description of illustrative embodiments of the invention is set forth below.

Brief Description of the Drawings

[0012] FIG. 1 shows a network system that includes three end point devices of a GRE tunnel.

[0013] FIG. 2 is a flowchart showing a process executed at an end point device of the GRE tunnel to update routing information in other end point devices.

[0014] FIG. 3 shows a routing update packet.

[0015] FIG. 4 shows a GRE header appended to the routing update packet.

[0016] FIG. 5 shows an encapsulated routing update packet including an outer delivery protocol header.

[0017] FIG. 6 is a flowchart showing a process executed at an end point device to process a routing update packet.

[0018] FIG. 7 is a diagram showing how packets are transmitted over the network system in one embodiment.

[0019] FIG. 8 is a flowchart showing a process executed at a GRE tunnel end point device to obtain a physical address of a remote end point device.

[0020] FIG. 9 shows an Address Resolution Protocol ("ARP") broadcast packet.

[0021] FIG. 10 shows a GRE header appended to the ARP broadcast packet.

[0022] FIG. 11 shows an encapsulated ARP broadcast packet, including an outer delivery protocol header.

[0023] FIG. 12, comprised of FIGs. 12a and 12b, is a flowchart showing a process executed at an end point device to process an encapsulated ARP broadcast

packet and to provide a reply to the ARP broadcast packet.

Description of the Preferred Embodiment

[0024] Referring to FIG. 1, a network system 10 is shown which includes devices 12, 14 and 16, local area networks ("LANs") 18 to 20, and intermediary network 22.

[0025] Intermediary network 22 may be any type of nenvork, such as a wide area network ("WAN") or the Internet, that supports IPv4 (Internet Protocol version 4), IP multicast routing, and IGMP (Internet Group Multicast Protocol). Examples of protocols that may be used to perform multieast routing are DVMRP (Distance Vector Multicast Routing Protocol), MOSPF (Multicast Open Shortest-Path First), and PIM (Protocol Independent Multicasting). Packets may also be "unicast" over intermediary network 22. Routes are distributed using protocols, such as RIP (Routing Information Protocol), OSPF (Open Shortest-Path First), and BGP (Border Gateway Protocol).

[0026] Included on intermediary network 22 is GRE tunnel 24. Intermediary network 22 has no knowledge, per se, of GRE tunnel 24. The GRE tunnel Is known only to the devices at its end points, namely devices 12, 14 and 16. GRE tunnel 24 passes encapsulated data packets between devices at tunnel end points 12, 14 and 16. Encapsulated packets may be sent to single, or multiple, tunnel end point devices.

[0027] Devices 12, 14 and 16 are coupled to corresponding LANs IS to 20. Each of LANs 18 to 20 supports IPv4 and one or more of the foregoing routing protocols for transmiting data packets between devices on the LAN (e.g., personal computer {"PC"} 29) and a GRE tunnel end paint. Since both LANs 18 to 20 and intermediary network 22 support IF, GRE encapsulation (described below) will be IP over IP.

[0028] Each tunnel has a multicast address. Each tunnel end point device a physical IP address and a logical IP address. The logical IP address is an IP address that is statically configured over a GRE tunnel end point device. The physical IP address is the network (IP) address of the end point device and is used by the delivery protocol to deliver data packets through GRE tunnels to remote devices.

[0029] Devices 12, 14 and 16 are routers, or other computing devices, which receive data packets (either from a GRE tunnel or a LAN) and which forward the data packets to their intended destinations (either via a GRE tunnel or on the LAN). For example, "local" device 12 receives payload data packets from PC 29 on LAN 18 and forwards those packets to "remote" device 14 via GRE tunnel 24. Similarly, device 12 receives packets from GRE tunnel 24 and forwards those packets onto LAN 18. Whether a device is local or remote is a matter of perspective only. For example, to device 14, devices 12 and 16 are remote.

[0030] Each device 12, 14 and 16 includes a memory 13 for storing computer instructions, and a processor 12a for executing those instructions to perform various functions, as shewn in blown-up view 30. For example, routing instructions 13c cause device 12 to forward routing packets in accordance with one or more of the routing protocols noted above. Dynamic GRE instructions 13b process GRE-encapsulated routing packets transmitted over GRE tunnel 24.

[0031] Memory 13 also stores an address table 13a and a routing table 13d. In this regard, each device has several associated addresses. For example, device 12 has an address 35 which includes a logical IP address 35a of "200.10.1.1", and a physical IP address 35b of "192.115.65.12". The multicast address 35c ("232.10.5.1") of GRE tunnel 24 is also shown, as are addresses of devices 14 and 16.

[0032] Routing table 13d stores network routing information, including the logical IP addresses of devices 12, 14, and 16. Routing table 13d is used by routing instructions 13c to route packets. Address table 13a stores the physical IP addresses of devices 12, 14 and 16 which map to corresponding logical IP addresses in routing table 13d.

[0033] If address table 13a needs to be updated with the physical IP address of devices 14 or 16, or if a logical/physical IP address mapping of device 12 needs to be updated in devices 14 and 16, dynamic GRE instructions 13b are executed. Dynamic GRE instructions 13b perform encapsulation and de-encapsulation, as described below. For broadcast and multicast packets, the destination IP address for such packets is a multicast address. For unicast packets, the destination address is a unicast address.

Determining a Device Logical Address

[0034] Referring to FIG. 2, a process 40, implemented by computer instructions, is shown for updating routing tables in remote GRE tunnel end point devices. For illustration's sake, device 14 is designated as the local GRE tunnel end point device which executes computer instructions to implement process 40.

[0035] Process 40 generates 42 a "routing update" packet 43 which holds network information 43a, including routing information such as the logical IP address of device 14 (see FIG. 3). Routing updates packets are multicast/broadcast packets (in the case of RIP and OSPF) or unicast packets (in the case of BGP).

[0036] Process 40 appends a GRE header 44 to routing update packet 43 (see FIG. 4). GRE header 44 includes a protocol type field 44a that specifies the protocol of packet 43, and a key present bit 44b that indicates if a tunnel key is enabled for the GRE tunnel.

[0037] A tunnel key is an integer from "0" to "0ffffffff" in GRE header 44. It specifies a unique tunnel identifier for each GRE tunnel. If a tunnel key is enabled, all outbound traffic over a GRE tunnel will have the tunnel key

in its GRE header. Inbound traffic over the GRE tunnel will be accepted only if the GRE tunnel key in the GRE header matches a tunnel key that is maintained in a memory on a tunnel end point device. Data packets that do not have the correct tunnel key are discarded.

[0038] Process 40 determines 45 whether to enable the tunnel key. If the tunnel key is enabled, process 40 appends 46 a tunnel key and a GRE header with key present bit 44b set to "1" (to indicate that the tunnel key is enabled). If the tunnel key is not enabled, process 40 appends 47 a GRE header with key present bit 44b set to "0" (to indicate that the tunnel key is not enabled). Tunnel keys need not be used in this embodiment

[0039] Process 40 appends 48 an outer IP delivery header 50 to packet 49 (see FIG. 5). IP delivery header 50 includes, as the destination address, a multicast address 50a of GRE tunnel 24. The IP delivery header includes, as the source address, the physical IP address 50b of device 14. The IP delivery header also includes a value in protocol field 50c to identify packet 54 as a GRE packet.

[0040] Process 40 forwards 52 GRE-encapsulated routing update packet 54 (FIG. 5) to muiticast address 50a specified in IP delivery header 50. At each remote tunnel end point device 12 and 16, the data packet is processed.

[0041] Referring to FIG. 6, a process 60 (in dynamic GRE instructions 13b) is executed by remote tunnel end point devices (from device 14's perspective), such as device 12, to handle routing updates received from device 14. Process 60 receives 62 the encapsulated data packet 54, determines 64 if the packet is a GRE packet (if not, the packet may be otherwise processed 66), strips 68 the outer IP delivery header 50 off of the received data packet, and determines 70 if the tunnel key is enabled based on key present bit 44b. If the tunnel key is enabled, process 60 compares 72 the tunnel key (not shown) in the packet to a tunnel key stored in its memory. If the two match 74 (or if a tunnel key was not enabled), process 60 strips 76 GRE header 44 from the packet 49, and reads 78 network information 43a from the packet. This network information 43a is stored in routing table 13d of device 12. This process enables distribution of routes that are reachable through a logical IP address of a GRE tunnel end point at device 14.

Obtaining a Device Physical Address

[0042] Referring to FIGs. 7 and 8, a process 80 is executed by instructions in device 12 to obtain the physical IP address of device 14. To begin, process 80 receives 82 a payload packet 83 from PC 29 on LAN 18. The payload packet is addressed to a PC 85 on remote LAN 19. Process 80 looks up a forwarding (delivery) address for PC 85 in routing table 13d. Based on the information in routing table 13d, process 80 determines that PC 85 is located at the other end of a GRE tunnel 24. Process 80 also determines the logical IP address of device 14 from routing table 13d. Process 80 determines 86 if the physical address of device 14 is known. This is done by searching through address table 13a.

[0043] If process 80 finds the physical IP address of device 14 in address table 13a, process 80 encapsulates 88 payload packet 83 (with a GRE header and outer IP delivery header) and forwards 108 encapsulated payload packet 87 through GRE tunnel 24 to device 14. If the physical IP address of device 14 is not found in address table 13a (or if device 12 has reason to believe that the address of device 14 has changed, e.g., due to network reconfiguration), process 80 determines 89 the physical IP address of device 14 dynamically.

[0044] To determine 89 the physical IP address of device 14, process 80 generates 90 an ARP broadcast packet 141 (see FIG. 9). ARP broadcast packet 141 includes the logical IP address 141a of device 14 as its payload. Process 80 encapsulates ARP broadcast packet 141 for transmission through GRE tunnel 24. Process 80 appends a GRE header 142 to ARP broadcast packet 141 (see FIG. 10). The GRE header 142 includes a protocol type field 142a that specifies the protocol of ARP broadcast packet 141. For ARP, the protocol type field is set to 0x806. GRE header 142 also includes a key present bit 142b, which indicates if a tunnel key is required for a GRE tunnel. A "0" in key present bit 142b indicates that no tunnel key is required and a "1" in key present bit 142b indicates that a tunnel key is required.

[0045] If the tunnel key is enabled 92, process 80 appends 94 the GRE header and tunnel key and sets key present bit 142b to "1"; otherwise it appends 96 the GRE header and sets key present bit 142b to "0". Process 80 appends 98 an outer IP delivery header 144 to packet 143 (see FIG. 11) to complete encapsulation. IP delivery header 144 includes, as the destination address, a multicast address 144a of GRE tunnel 24. IP delivery header 144 includes, as the source address, the physical IP address 144b of device 12. IP delivery header 144b also includes a value in a protocol field 144c which signifies that the packet is a GRE packet.

[0046] Process 80 forwards 100 the encapsulated ARP broadcast packet 145 (FIGs. 7 and 11) to multicast address 144a specified in IP delivery header 144. Device 14 (which is a member of the multicast group for the multicast address) receives encapsulated ARP broadcast packet 145 and processes it as described in FIG. 12 below. In response, device 14 forwards an encapsulated ARP reply packet 146 (FIG. 7) to device 12, which includes the physical IP address of device 14. Process 80 receives 102 the ARP reply packet and reads the physical IP address of device 14.

[0047] Process 80 updates 104 the address table 13a in device 12 to include the physical IP address of device 14. The physical IP address of device 14 is indexed to its logical IP address so that subsequent data packets can be forwarded by referring to the address table.

[0048] Once both the logical and physical IP address-

es of device 14 are known, process 80 encapsulates 106 the payload packet 83 and forwards 108 the encapsulated payload packet 87 through GRE tunnel 24 to the physical IP address of device 14 (received in 102). Encapsulation 106 of the payload packet 83 is identical to the encapsulation process described above, except that the physical IP address of device 14 is used as the IP delivery header destination address instead of multicast address 144a. At device 14, the encapsulated packet 87 is de-encapsulated and the de-encapsulated payload packet 147 is transmitted to PC 85.

[0049] Referring to FIG. 12, a process 150 is shown by which device 14 determines whether to issue a reply to the encapsulated ARP broadcast packet 145 from device 12.

[0050] Process 150 receives 152 the encapsulated ARP broadcast packet 145 from device 12 via GRE tunnel 24. Process 150 determines 154, based on the value in the packet's protocol field 144c, whether the data packet is a GRE packet. If the packet is not a GRE packet, device 14 may use it in other processing 156.

[0051] If the packet is a GRE packet, device 14 strips 158 the IP delivery header 144 off the packet and reads the physical IP address 144b of device 12. Device 14 also checks 160 (using the key present bit in the GRE header) whether a tunnel key has been enabled. If so, device 14 compares 162 the tunnel key in the data packet to a tunnel key stored in its memory. If the tunnel keys do not match 164, process 150 discards 168 the packet and returns. If the tunnel keys match 164, or if it was determined 160 that the tunnel key was not enabled, process 150 strips 166 the GRE header 142 from the packet and reads 170 the logical IP address 141a from the payload of the ARP broadcast packet. If the logical IP address 141a from the ARP broadcast packet does not match 172 the logical address of device 14, the packet is discarded 168. If the two match, process 150 prepares 174 an ARP reply packet which includes the physical IP (unicast) address of device 14 as its payload.

[0052] The ARP reply packet is encapsulated 176 for transmission to device 12 over GRE tunnel 24. The encapsulation process is similar to that described above. However, the physical IP address of device 12 (144b from encapsulated ARP broadcast packet 145) is used as the destination address in the IP delivery header of encapsulated ARP reply packet 147. The encapsulated ARP reply packet 147 is forwarded 178 to device 12 over GRE tunnel 24. Device 12 processes the reply packet as described in FIG. 6 above to read the physical IP address of device 14 therefrom.

[0053] Other embodiments are within the scope of the following claims. For example, the invention can be used with protocols and networks other than those described above. In addition, the invention can be used on any type of networkable device, not just PCs and routers.

Claims

1. A method of obtaining an end point address of a generic routing encapsulation (GRE) tunnel, comprising:

   forwarding a data packet through the GRE tunnel to a remote GRE tunnel end point device; and

   receiving a reply from the remote GRE tunnel end point device, the reply including a physical address of the remote GRE tunnel end point device.

2. The method of claim 1, wherein the method is performed by a local GRE tunnel end point device; and

   further comprises updating a table on the local GRE tunnel end point device to include the physical address of the remote GRE tunnel end point device.

3. The method of claim 2, wherein the reply includes a unicast address of the remote GRE tunnel end point device.

4. The method of claim 1, wherein the data packet comprises an address resolution protocol (ARP) packet; and

   wherein the ARP packet includes a logical address of the remote GRE tunnel end point device.

5. The method of claim 1, wherein the reply comprises a GRE-encapsulated data packet with the physical address of the remote GRE tunnel end point device as a payload.

6. A method of determining an end point of a generic routing encapsulation (GRE) tunnel, comprising:

   receiving a data packet at a device;

   identifying the data packet as a GRE packet;

   determining an address of the end point of the GRE tunnel using the data packet; and

   storing the address in a table on the device.

7. The method of claim 6, wherein identifying comprises searching a header of the data packet for a value indicative of a GRE packet.

8. The method of claim 6, wherein the address of the end point comprises a logical address of the end point.

9. The method of claim 6, wherein the device is a router, and the data packet comprises a routing update packet.

10. A computer program stored on a computer-readable medium for obtaining an end point address of a

generic routing encapsulation (GRE) tunnel, the computer program comprising instructions that cause a computer to:

forward a data packet through the GRE tunnel to a remote GRE tunnel end point device; and
receive a reply from the remote GRE tunnel end point device, the reply including a physical address of the remote GRE tunnel end point device.

11. A computer program stored on a computer-readable medium for determining an end point of a generic routing encapsulation (GRE) tunnel, the computer program comprising instructions that cause a computer to:

receive a data packet at a device;
identify the data packet as a GRE packet;
determine an address of the end point of the GRE tunnel using the data packet; and
store the address in a table on the device.

12. An apparatus for obtaining an end point address of a generic routing encapsulation (GRE) tunnel, the apparatus comprising a processor which executes computer code to:

forward a data packet through the GRE tunnel to a remote GRE tunnel end point device; and
receive a reply from the remote GRE tunnel end point device, the reply including a physical address of the remote GRE tunnel end point device.

13. An apparatus for determining an end point of a generic routing encapsulation (GRE) tunnel, the apparatus comprising a processor which executes computer code to:

receive a data packet at a device coupled to the processor;
identify the data packet as a GRE packet;
determine an address of the end point of the GRE tunnel using the data packet; and
store the address in a cable on the device.

14. A network system comprising:

a first device in a multicast group;
a second device in the multicast group; and
a generic routing encapsulation (GRE) tunnel configured over a network between a first end point at the first device and a second end point at the second device;
wherein the first device forwards a data packet through the GRE tunnel to devices in the multicast group, the data packet requesting an address; and
wherein the second device issues a reply to the first device via the GRE tunnel, the reply including an address of the second device.

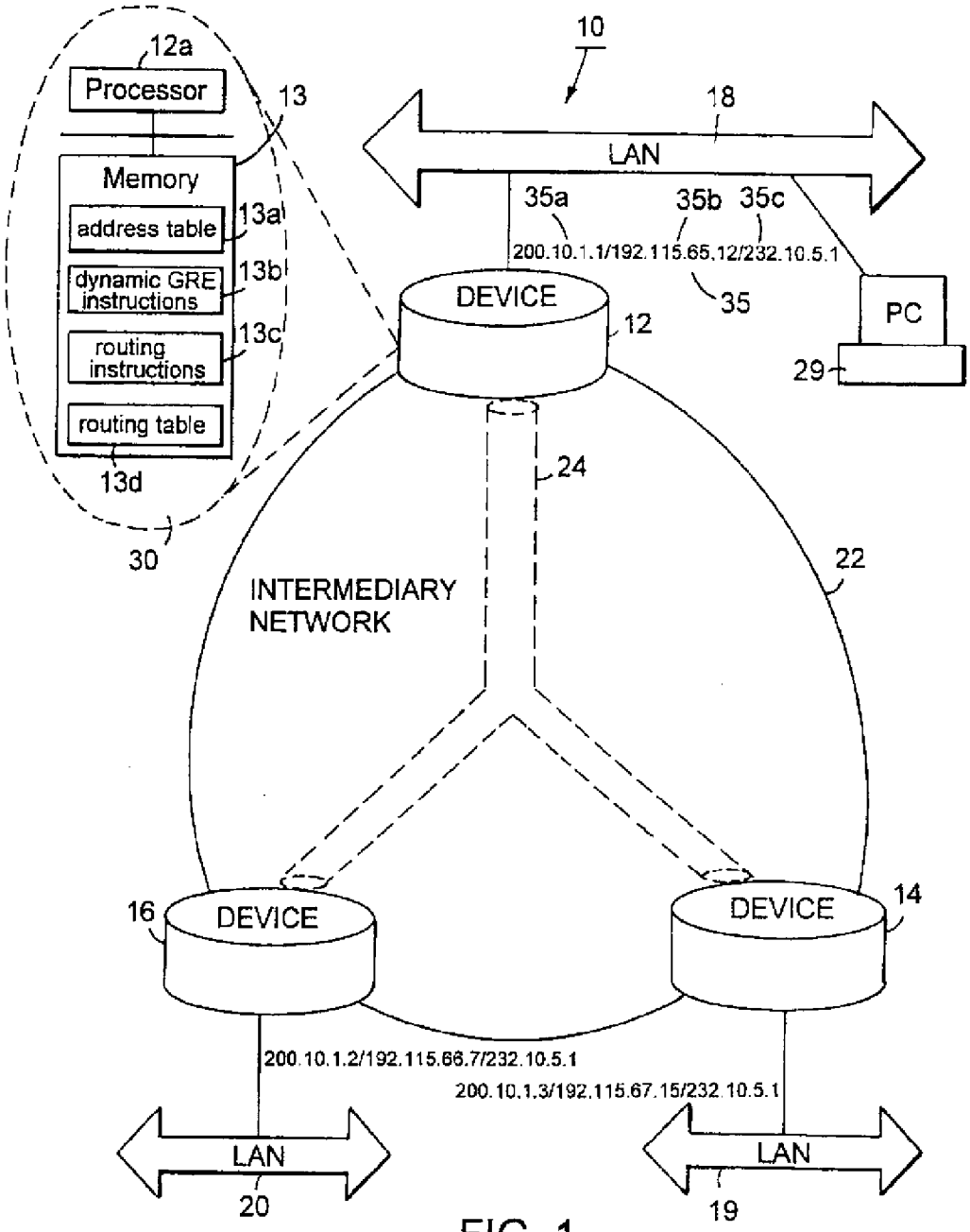

10
12a
Processor
13
Memory
address table
13a
dynamic GRE instructions
13b
routing instructions
13c
routing table
13d
30
18
LAN
35a
35b
35c
200.10.1.1/192.115.65.12/232.10.5.1
35
DEVICE
12
PC
29
24
22
INTERMEDIARY NETWORK
16
DEVICE
14
DEVICE
200.10.1.2/192.115.66.7/232.10.5.1
200.10.1.3/192.115.67.15/232.10.5.1
LAN
20
LAN
19

FIG. 1

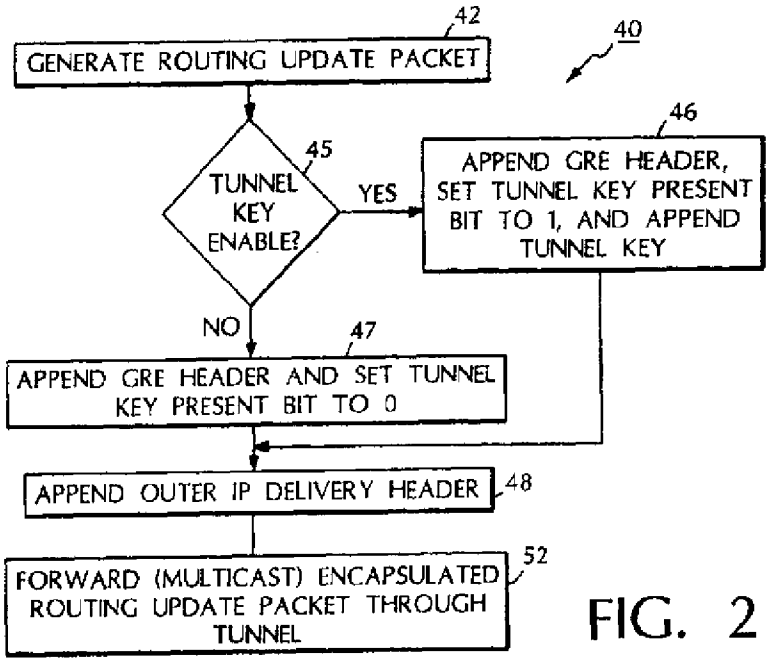


FIG. 2

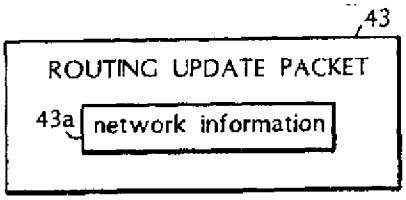


FIG. 3

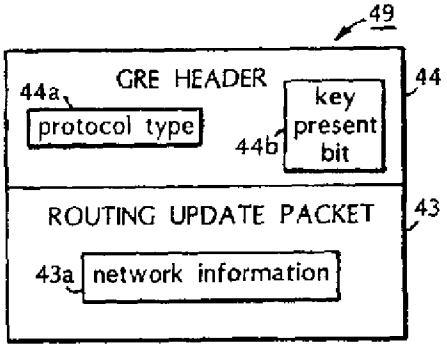


FIG. 4

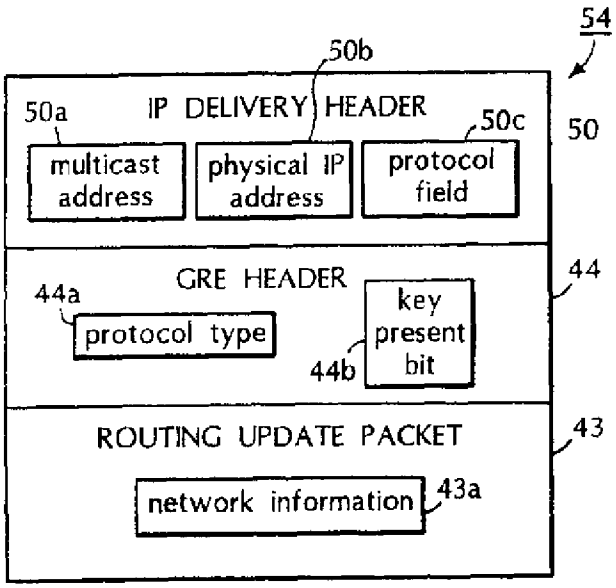

54
50b
50a
IP DELIVERY HEADER
50c
50
multicast address
physical IP address
protocol field
GRE HEADER
44
44a
protocol type
key present bit
44b
ROUTING UPDATE PACKET
43
network information
43a

FIG. 5

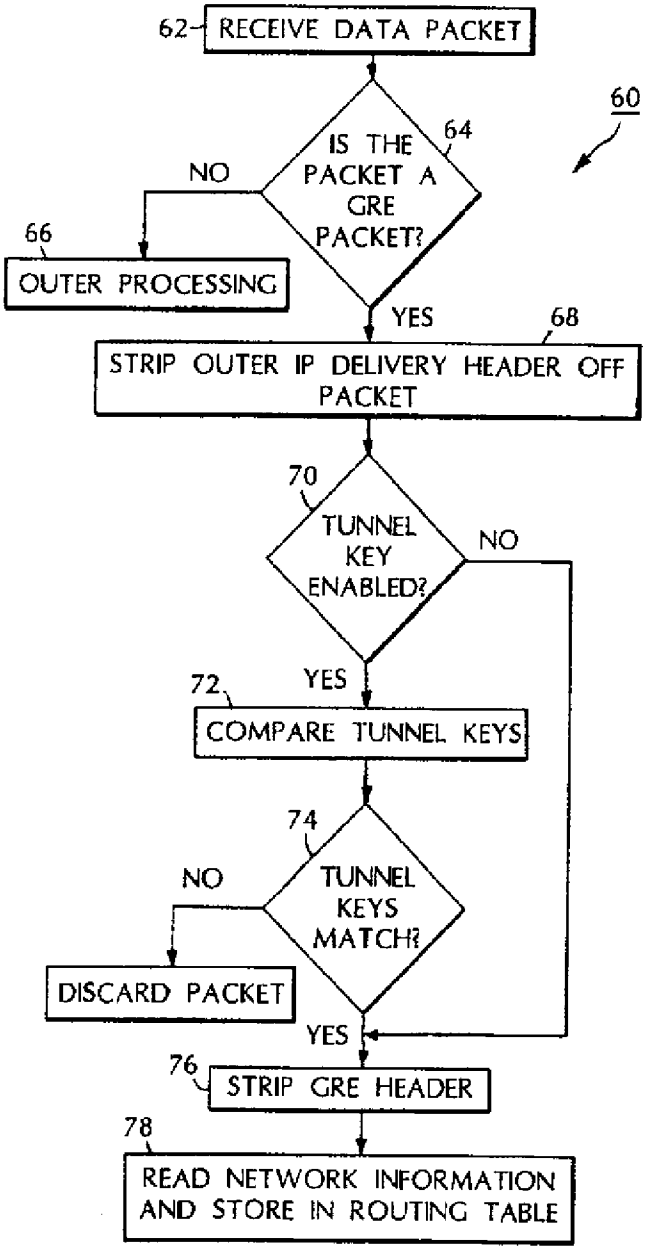

62
RECEIVE DATA PACKET
60
64
IS THE PACKET A GRE PACKET?
NO
66
OUTER PROCESSING
YES
68
STRIP OUTER IP DELIVERY HEADER OFF PACKET
70
TUNNEL KEY ENABLED?
NO
YES
72
COMPARE TUNNEL KEYS
74
TUNNEL KEYS MATCH?
NO
DISCARD PACKET
YES
76
STRIP GRE HEADER
78
READ NETWORK INFORMATION AND STORE IN ROUTING TABLE

FIG. 6

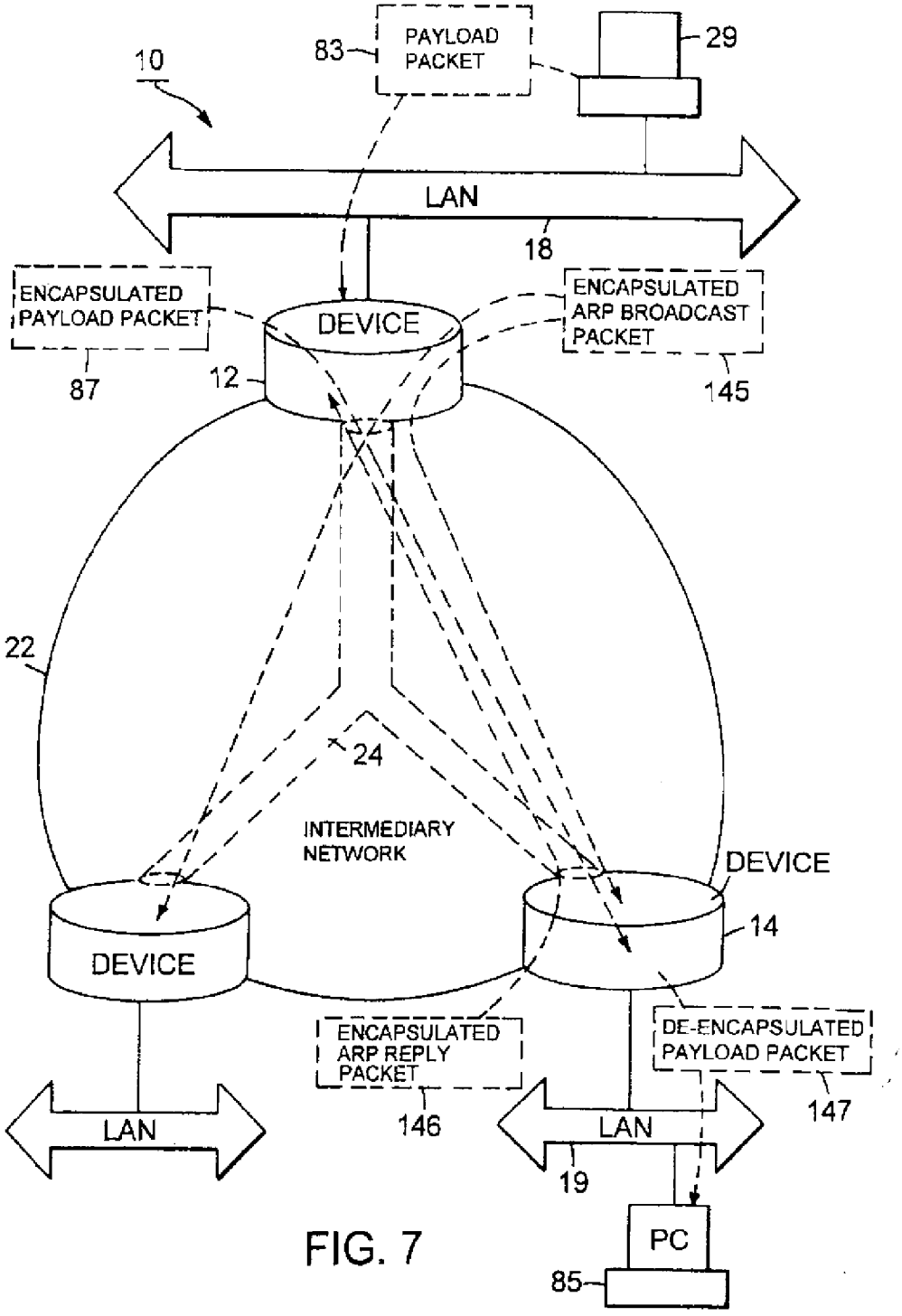

10
83
PAYLOAD PACKET
29
LAN
18
ENCAPSULATED PAYLOAD PACKET
87
DEVICE
12
ENCAPSULATED ARP BROADCAST PACKET
145
22
24
INTERMEDIARY NETWORK
DEVICE
14
DEVICE
ENCAPSULATED ARP REPLY PACKET
146
DE-ENCAPSULATED PAYLOAD PACKET
147
LAN
LAN
19
PC
85

FIG. 7

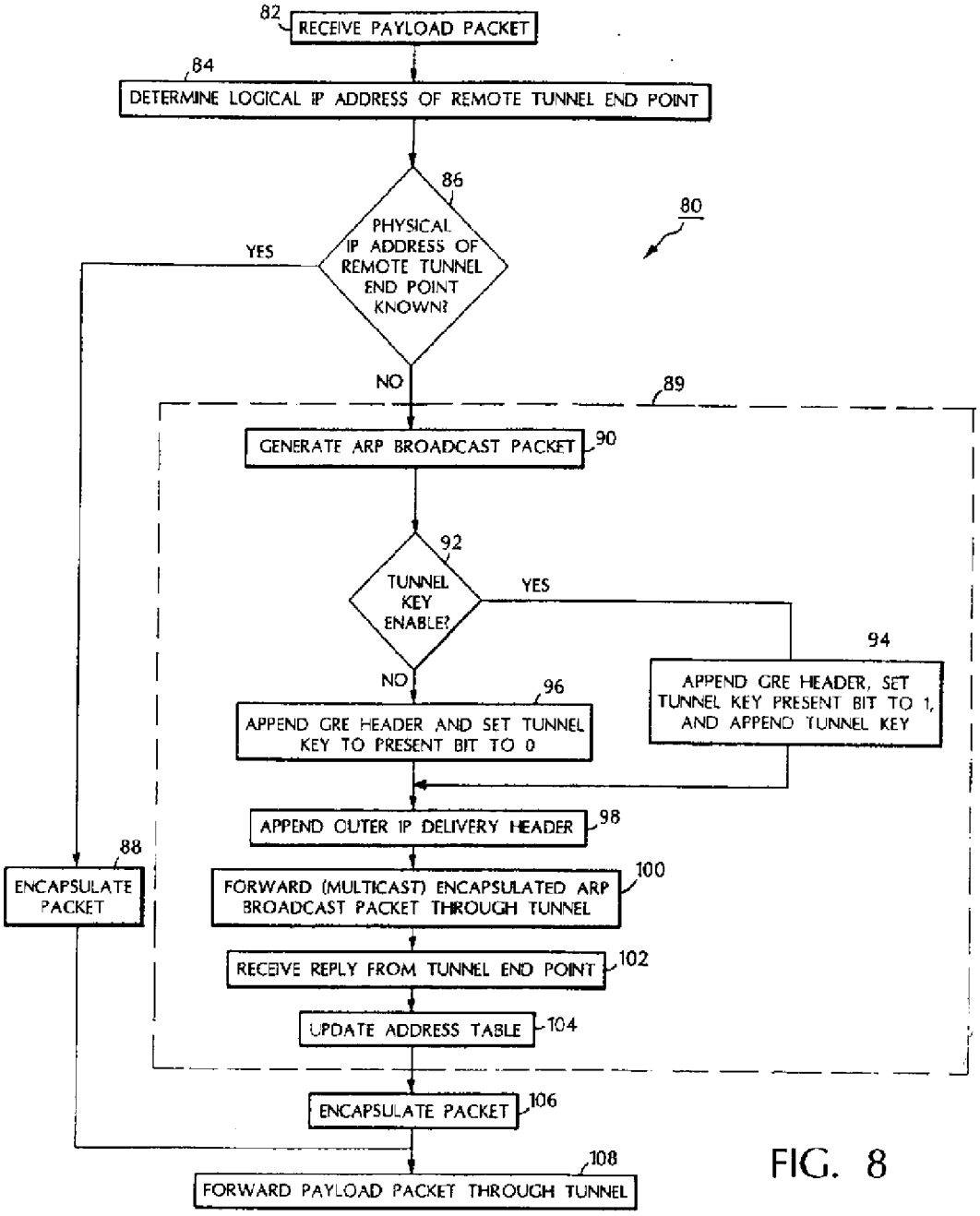

82
RECEIVE PAYLOAD PACKET
84
DETERMINE LOGICAL IP ADDRESS OF REMOTE TUNNEL END POINT
86
PHYSICAL IP ADDRESS OF REMOTE TUNNEL END POINT KNOWN?
YES
NO
80
89
GENERATE ARP BROADCAST PACKET
90
92
TUNNEL KEY ENABLE?
YES
NO
94
APPEND GRE HEADER, SET TUNNEL KEY PRESENT BIT TO 1, AND APPEND TUNNEL KEY
96
APPEND GRE HEADER AND SET TUNNEL KEY TO PRESENT BIT TO 0
98
APPEND OUTER IP DELIVERY HEADER
88
ENCAPSULATE PACKET
100
FORWARD (MULTICAST) ENCAPSULATED ARP BROADCAST PACKET THROUGH TUNNEL
102
RECEIVE REPLY FROM TUNNEL END POINT
104
UPDATE ADDRESS TABLE
106
ENCAPSULATE PACKET
108
FORWARD PAYLOAD PACKET THROUGH TUNNEL

FIG. 8

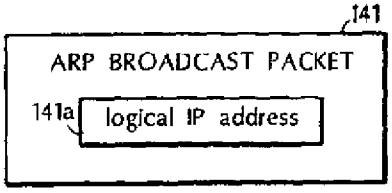


FIG. 9

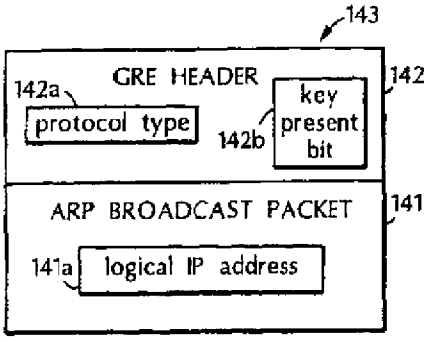


FIG. 10

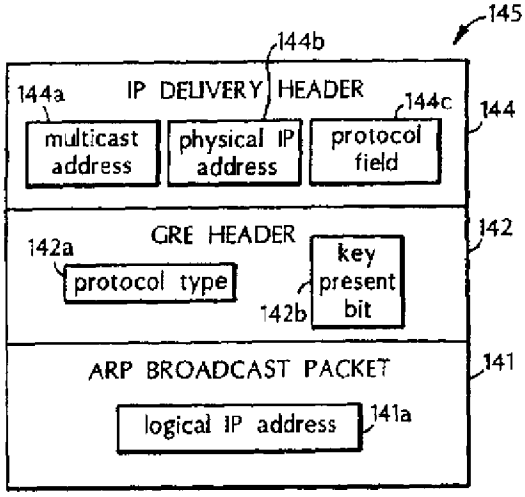


FIG. 11

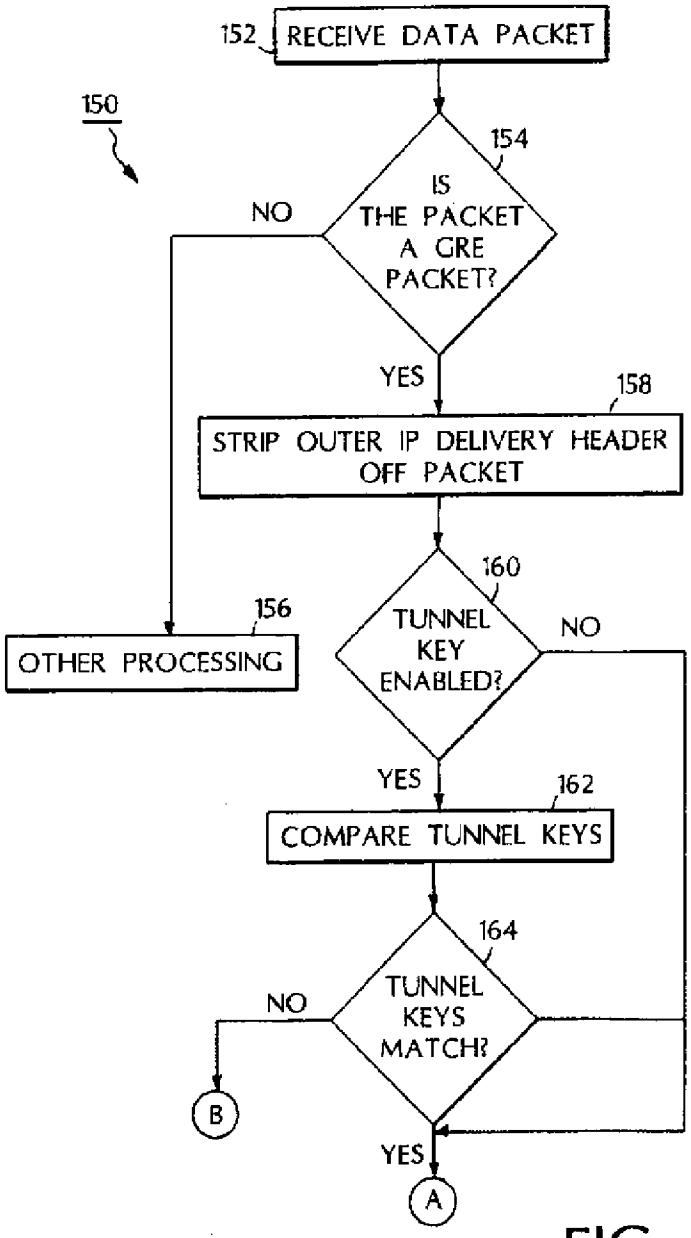


FIG. 12A

FIG. 12B

FIG. 12

FIG. 12A

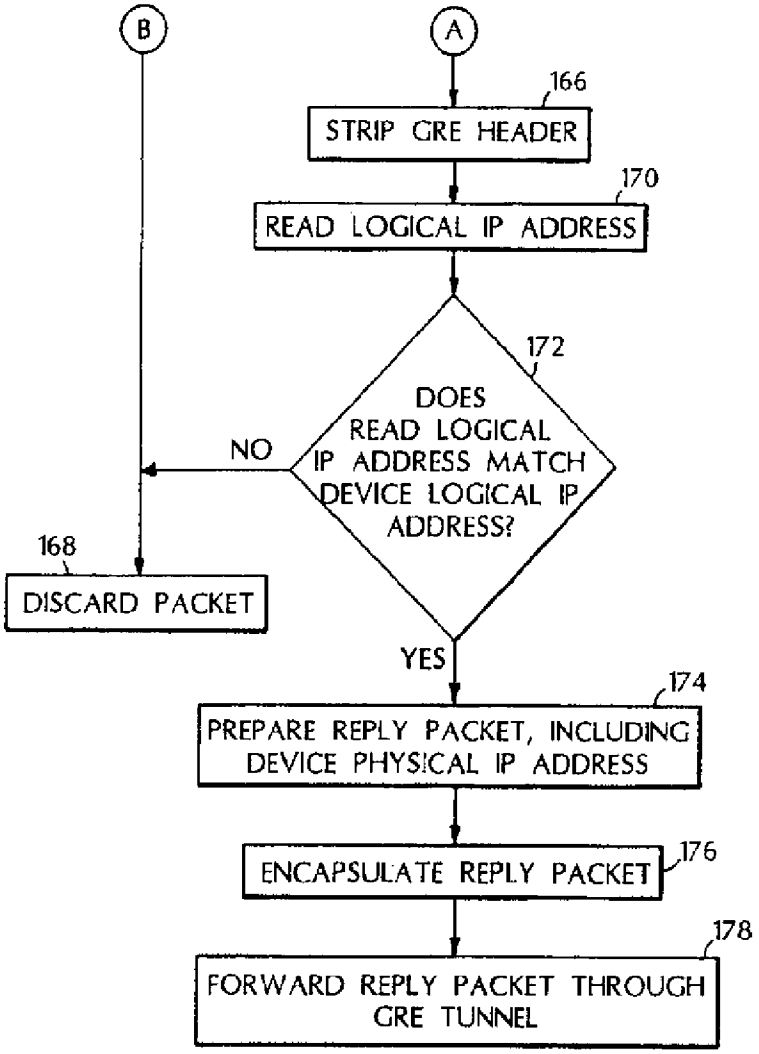

B
A
166
STRIP GRE HEADER
170
READ LOGICAL IP ADDRESS
172
DOES READ LOGICAL IP ADDRESS MATCH DEVICE LOGICAL IP ADDRESS?
NO
168
DISCARD PACKET
YES
174
PREPARE REPLY PACKET, INCLUDING DEVICE PHYSICAL IP ADDRESS
176
ENCAPSULATE REPLY PACKET
178
FORWARD REPLY PACKET THROUGH GRE TUNNEL

FIG. 12B

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 213 943 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
12.06.2002 Bulletin 2002/24

(51) Int Cl.7: **H04Q 7/38**

(21) Application number: **01306907.5**

(22) Date of filing: **14.08.2001**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **11.12.2000 US 734148**

(71) Applicant: **LUCENT TECHNOLOGIES INC.**
Murray Hill, New Jersey 07974-0636 (US)

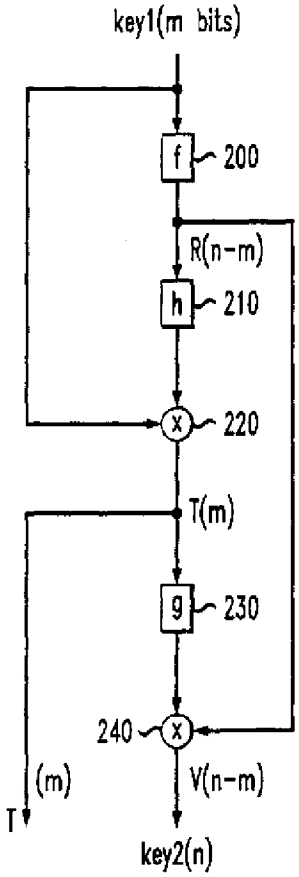
(72) Inventor: **Patel, Sarvar**
Montville, New Jersey 07045 (US)

(74) Representative:
Buckley, Christopher Simon Thirsk et al
Lucent Technologies NS UK Limited,
Intellectual Property Division,
5 Mornington Road
Woodford Green, Essex IG8 0TU (GB)

(54) Key conversion system and method

(57) The present invention is a key conversion system for deterministically and reversibly converting a first key value of a first communications system into a second key value of a second communication system. For example, the key conversion system generates a first intermediate value from at least a portion of the first key value using a first random function. At least a portion of the first intermediate value is provided to a second random function to produce a second value. An exclusive-or is performed on at least a portion of the first key value and at least a portion of the second value to generate a second intermediate value. At least a portion of the second intermediate value is provided to a third random function to produce a third value. By performing an exclusive-or on at least a portion of the third value and at least a portion of the first intermediate value, the key conversion system produces at least a first portion of the second key value, and at least a second portion of the second key value is produced as the second intermediate value.

FIG. 11



EP 1 213 943 A1

Description

BACKGROUND OF THE INVENTION

1. Field of The Invention

[0001] The present invention relates to communications; more specifically, the conversion of keys for first and second communications systems as the wireless unit roams between the first and second communications systems.

2. Description of Related Art

[0002] FIG. 1 depicts a schematic diagram of first and second wireless communications systems which provide wireless communications service to wireless units (e.g., wireless units 12a-c) that are situated within the geographic regions 14 and 16, respectively. A Mobile Switching Center (e.g. MSCs 20 and 24) is responsible for, among other things, establishing and maintaining calls between the wireless units, calls between a wireless unit and a wireline unit (e.g., wireline unit 25), and/or connections between a wireless unit and a packet data network (PDN), such as the internet. As such, the MSC interconnects the wireless units within its geographic region with a public switched telephone network (PSTN) 28 and/or a packet data network (PDN) 29. The geographic area serviced by the MSC is divided into spatially distinct areas called "cells." As depicted in FIG. 1, each cell is schematically represented by one hexagon in a honeycomb pattern; in practice, however, each cell has an irregular shape that depends on the topography of the terrain surrounding the cell.

[0003] Typically, each cell contains a base station (e.g. base stations 22a-e and 26a-e), which comprises the radios and antennas that the base station uses to communicate with the wireless units in that cell. The base stations also comprise the transmission equipment that the base station uses to communicate with the MSC in the geographic area. For example, MSC 20 is connected to the base stations 22a-e in the geographic area 14, and an MSC 24 is connected to the base stations 26a-e in the geographic region 16. Within a geographic region, the MSC switches calls between base stations in real time as the wireless unit moves between cells, referred to as call handoff. Depending on the embodiment, a base station controller (BSC) can be a separate base station controller (BSC) (not shown) connected to several base stations or located at each base station which administers the radio resources for the base stations and relays information to the MSC.

[0004] The MSCs 20 and 24 use a signaling network 32, such as a signaling network conforming to the standard identified as TIA/EIA-41-D entitled "Cellular Radiotelecommunications Intersystem Operations," December 1997 ("IS-41"), which enables the exchange of information about the wireless units which are roaming within the respective geographic areas 14 and 16. For example, a wireless unit 12a is roaming when the wireless unit 12a leaves the geographic area 14 of the MSC 20 to which it was originally assigned (e.g. home MSC). To ensure that a roaming wireless unit can receive a call, the roaming wireless unit 12a registers with the MSC 24 in which it presently resides (e.g., the visitor MSC) by notifying the visitor MSC 24 of its presence. Once a roaming wireless unit 12a is identified by a visitor MSC 24, the visitor MSC 24 sends a registration request to the home MSC 20 over the signaling network 32, and the home MSC 20 updates a database 34, referred to as the home location register (HLR), with the identification of the visitor MSC 24, thereby providing the location of the roaming wireless unit 12a to the home MSC 20.

[0005] After a roaming wireless unit is authenticated, the home MSC 20 provides to the visitor MSC 24 a customer profile which indicates the features available to the roaming wireless unit, such as call waiting, caller id, call forwarding, three-way calling, and international dialing access. Upon receiving the customer profile, the visitor MSC 24 updates a database 36, referred to as the visitor location register (VLR), to provide the same features as the home MSC 20. The HLR, VLR and/or the authentication center (AC) can be co-located at the MSC or remotely accessed.

[0006] If a wireless unit is roaming between wireless communications systems using different wireless communications standards, providing the wireless unit with the same features and services in the different wireless communications systems is complex if even feasible. There are currently different wireless communication standards utilized in the U.S., Europe, and Japan. The U.S. currently utilizes two major wireless communications systems with differing standards. The first system is a time division multiple access system (TDMA) and is governed by the standard known as IS-136, the second system is a code division multiple access (CDMA) system governed by the standard known as IS-95. Both communication systems use the standard known as IS-41 for intersystem messaging, which defines the authentication procedure.

[0007] In TDMA, users share a frequency band, each user's speech is stored, compressed and transmitted as a quick packet, using controlled time slots to distinguish them, hence the phrase "time division". At the receiver, the packet is decompressed. In the IS-136 protocol, three users share a given carrier frequency. In contrast, CDMA uses a unique code to "spread" the signal across the wide area of the spectrum (hence the alternative name - spread spectrum), and the receiver uses the same code to recover the signal from the noise. A very robust and secure channel can be established, even for an extremely low-power signal. Further, by using different codes, a number of different channels can simultaneously share the same carrier signal without interfering with each other. Both CDMA and TDMA systems are defined for a Second Generation (2G) and Third Gen-

eration (3G) phases with differing requirements for user information privacy or confidentiality.

[0008] Europe utilizes the Global System for Mobiles (GSM) network as defined by the European Telecommunications Standard Institute (ETSI). GSM is a TDMA standard, with 8 users per carrier frequency. The speech is taken in 20 msec windows, which are sampled, processed, and compressed. GSM is transmitted on a 900 MHz carrier. There is an alternative system operating at 1.8 GHz (DCS 1800), providing additional capacity, and is often viewed as more of a personal communication system (PCS) than a cellular system. In a similar way, the U.S. has also implemented DCS-1900, another GSM system operating on the different carrier of 1.9 GHz. Personal Digital Cellular (PDC) is the Japanese standard, previously known as JDC (Japanese Digital Cellular). PDC is a TDMA standard similar to the U.S. standard known as IS-54 protocol.

[0009] The GSM network utilizes a removable user identification module (UIM) which is a credit card size card which is owned by a subscriber, who slides the UIM into any GSM handset to transform it into "their" phone. It will ring when their unique phone number is dialed, calls made will be billed to their account; all options and services connect; voice mail can be connected and so on. People with different UIMs can share one "physical" handset, turning it into several "virtual" handsets, one per UIM. Similar to the U.S. systems, the GSM network also permits "roaming", by which different network operators agree to recognize (and accept) subscribers from other wireless communications systems or networks, as wireless units (or UIMs) move. So, British subscribers can drive through France or Germany and use their GSM wireless unit to make and receive calls (on their same UK number), with as much ease as an American businessman can use a wireless unit in Boston, Miami, or Seattle, within any one of the U.S. wireless communications system. The GSM system is defined as a Second Generation (2G) system.

[0010] The third generation (3G) enhancement of the GSM security scheme is defined in the Universal Mobile Telecommunications Service (UMTS) set of standards, and specifically for the security in the standard identified as 3GPP TS-33.102 "Security Architecture" specifications. This security scheme with slight variations will be used as a basis for the worldwide common security scheme for all 3G communications systems, including UMTS, TDMA, and CDMA.

[0011] The 2G GSM authentication scheme is illustrated in FIG. 2. This authentication scheme includes a home location register (HLR) 40, a visiting location register (VLR) 50, and a wireless unit or mobile terminal (MT) 60, which includes a UIM 62. When the mobile terminal 60 places a call, a request is sent to the home location register 40, which generates an authentication vector AV, also called "triplet" (RAND, SRES, K_c) from a root key K_i. The triplet includes a random number RAND, a signed response SRES, and a session key K_c. The triplet is provided to the visiting location register 50, which passes the random number RAND to the mobile terminal 60. The UIM 62 receives the random number RAND, and utilizing the root key K_i, the random number RAND, and an algorithm A3, calculates a signed response SRES. The UIM 62 also utilizes the root key K_i and the random number RAND, and an algorithm A8 to calculate the session key K_c. The SRES, calculated by the UIM 62, is returned to the visiting location register 50, which compares this value from the SRES received from the home location register 40, in order to authenticate the subscriber using the mobile terminal 30.

[0012] In the GSM "challenge/response" authentication system, the visiting location register 50 never receives the root key K_i being held by the UIM 32 and the home location register 40. The VLR 50 also does not need to know the authentication algorithms used by the HLR 40 and UIM 62. Also, in the GSM authentication scheme, the triplet must be sent for every phone call by the home location register 40. RAND is 128 bits, SRES is 32 bits, and K_c is 64 bits, which is 224 bits of data for each request, which is a significant data load. The main focus of this description is the 64 bits long K_c session ciphering key which is used for user information confidentiality. When the mobile terminal roams into another serving system while in the call, the session key K_C is forwarded from the old VLR to the new target serving system.

[0013] FIG. 3 shows the UMTS security scheme which is an enhancement to the 2G GSM scheme. Similar to the GSM scheme, when the mobile terminal 90 places a call, a request is sent to the home location register 70, which sends an authentication vector - AV to the Visited Location Register (VLR) 80 which contains five elements instead of the three elements of a triplet, and therefore is called "quintuplet". This vector contains the 128 bit RAND, the 64 bits SRES, the AUTN value which carries the authentication signature of the home network, and two session security keys: the 128 bit ciphering key CK and the 128 bit integrity key IK. These latter two keys, CK and IK, are the focus of this description.

[0014] The vector is provided to the visiting location register 80, which passes the random number RAND and the AUTN to the mobile terminal 90. The UIM 92 receives the random number RAND, and utilizing the root key K_i, the random number RAND, and an defined algorithmic functions, validates the AUTN and calculates a signed response SRES. The UIM 92 also utilizes the root key K_i and the random number RAND and defined algorithmic functions to calculate the session keys CK and IK. The SRES, calculated by the UIM 92, is returned to the visiting location register 80, which compares this value from the SRES received from the home location register 70 in order to authenticate the subscriber using the mobile terminal 90. A focus of this description are the 128 bits long session ciphering key CK and 128 bits long session integrity key IK which are used for

user information confidentiality and session integrity protection. Once the subscriber is successfully authenticated, the VLR 80 activates the CK and IK received in this authentication vector. If the mobile terminal roams into another serving system while on the call, the CK and IK are sent to the new target serving system.

[0015] The 2G IS-41 authentication scheme, used in U.S. TDMA and CDMA systems, is illustrated in FIG. 4. This authentication scheme involves a home location register (HLR) 100, a visiting location register (VLR) 110, and a mobile terminal (MT) 120, which can include a UIM 122. The root key, known as the A_key, is stored only in the HLR 100 and the UIM 122. There is a secondary key, known as Shared Secret Data SSD, which is sent to the VLR 110 during roaming. SSD is generated from the A_key using a cryptographic algorithm. The procedure for generating the SSD is described elsewhere and is known to those skilled in the art. When the MT 120 roams to a visiting network, the VLR 110 sends an authentication request to the HLR 100, which responds by sending that subscriber's SSD. Once the VLR 110 has the SSD, it can authenticate the MT 120 independently of the HLR 100, or with the assistance of the HLR 100 as is known to those skilled in the art. The VLR 110 sends a random number RAND to the UIM 122 via the MT 120, and the UIM 122 calculates the authentication response (AUTHR) using RAND and the stored value of SSD in UIM 122. AUTHR is returned to the VLR 110, which checks it against the value of AUTHR that it has independently calculated in the same manner. If the two AUTHR values match, the MT 120 is declared valid. This process repeats when the wireless unit attempts to access the system, for instance, to initiate a call, or to answer a page when the call is received.

[0016] In these cases, the session security keys are also generated. To generate session security keys, the internal state of the computation algorithm is preserved after the authentication calculation. Several session security keys are then calculated by the UIM 122 and the VLR 110 using the current value of SSD. Specifically, the 520 bits Voice Privacy Mask (VPM) is computed, which is used for concealing the TDMA speech data throughout the call. This VPM is derived at the beginning of the call by the UIM and VLR, and, if the mobile roams into another serving system during the call, the VPM is sent to the new serving system by the VLR. When the call is concluded, the VPM is erased by both the UIM and the serving VLR. Likewise, the 64 bits Signaling Message Encryption Key (SMEKEY) is computed, which is used for encrypting the TDMA signaling information throughout the call. This SMEKEY is derived at the beginning of the call by the UIM and VLR, and, if the mobile roams into another serving system during the call, the SMEKEY is sent to the new serving system by the VLR. When the call is concluded, the SMEKEY is erased by both the UIM and the serving VLR.

[0017] The 2G CDMA scheme uses a similar method of key distribution, except, instead of the 520 bits VPM, it is using the 42 Least Significant Bits (LSB) of the VPM as a seed into the Private Long Code Mask (PLCM). This PLCM is used as an additional scrambling mask for the information before its spreading. The 42-bit PLCM is consistent throughout the call and is sent to the new serving system by the VLR if the mobile roams into another serving system. The SMEKEY is used in the same way as in the TDMA based scheme.

[0018] The IS-41 3G security scheme uses the UMTS security scheme, which is based on the delivery of the 128-bits ciphering key CK and 128-bits integrity key IK to the visited system VLR, while the same keys are computed by the UIM.

[0019] Key conversions as a wireless unit roams between communications systems should be performed in a way that even if lower security of 2G schemes and algorithms is compromised and partial keys are recovered by the intruder, the 3G session keys would still maintain the same level of security. Such conversions will allow a subscriber to "roam globally" maintaining the security of communications data and integrity of communications session.

SUMMARY OF THE INVENTION

[0020] The present invention is a key conversion system for deterministically and reversibly converting a first key value of a first communications system into a second key value of a second communication system. For example, the key conversion system generates a first intermediate value from at least a portion of the first key value using a first random function. At least a portion of the first intermediate value is provided to a second random function to produce a second value. An exclusive-or is performed on at least a portion of the first key value and at least a portion of the second value to generate a second intermediate value. At least a portion of the second intermediate value is provided to a third random function to produce a third value. By performing an exclusive-or on at least a portion of the third value and at least a portion of the first intermediate value, the key conversion system produces at least a first portion of the second key value, and at least a second portion of the second key value is produced as the second intermediate value. The key conversion system is deterministic in that, given a first key value, a wireless unit and the wireless communications system will determine the same second key value without requiring an exchange of information.

[0021] The key conversion system is reversible or bi-directional in that, if the wireless unit is handed off back to the first communications system, the second key value of the second communications system is converted back to the first key value of the first communications system. For example, the key conversion system provides the at least second portion of the second key value to the third random function to produce the third value. The first intermediate value is generated by performing

an exclusive-or on the first portion of the second key value and the third value. Using the second random function, the key conversion system generates the second value from the first intermediate value and produces at least a portion of the first key by performing an exclusive-or on the second value and the second portion of the second key value. The key conversion system provides improved security because even if almost all of the second key value is known, the first key value cannot easily be recovered. Similarly, if almost all of the first key value is known, the second key value is not easily recovered.

BRIEF DESCRIPTION OF THE DRAWINGS

[0022] Other aspects and advantages of the present invention may become apparent upon reading the following detailed description and upon reference to the drawings in which:

FIG. 1 shows a general diagram of wireless communications systems for which the key conversion system according to the principles of the present invention can be used;

FIG. 2 is a block diagram illustrating the basic components of the prior art 2G global system for mobiles (GSM) network and security messages transmitted in the 2G GSM network;

FIG. 3 is a block diagram illustrating the basic components of the prior art 3G UMTS network and messages transmitted in the 3G UMTS network;

FIG. 4 is a block diagram illustrating the basic components of the prior art 2G IS-41 network and messages transmitted in the prior art 2G IS-41 network;

FIG. 5 is a block diagram illustrating how a user roams from a 2G TDMA network into a generic 3G network;

FIG. 6 is a block diagram illustrating how a user roams from a generic 3G network into a 2G TDMA network;

FIG. 7 is a block diagram illustrating how a user roams from a 2G CDMA network into a generic 3G network;

FIG. 8 is a block diagram illustrating how a user roams from a generic 3G network into a 2G CDMA network;

FIG. 9 is a block diagram illustrating how a user roams from a 2G GSM network into a generic 3G network;

FIG. 10 is a block diagram illustrating how a user roams from a generic 3G network into a 2G GSM network;

FIG. 11 is a flow diagram of an embodiment of the forward conversion for the key conversion system according to principles of the present invention; and

FIG. 12 is a flow diagram of an embodiment of the reverse conversion for the key conversion system according to principles of the present invention.

DETAILED DESCRIPTION

[0023] An illustrative embodiment of the key conversion system according to the principles of the present invention is described below which provides an improved key conversion for a wireless unit which roams between first and second wireless communications systems. The key conversion system deterministically and reversibly converts an m bit key value of a first communications system into an n-bit key value of a second communication system. In certain embodiments, the key conversion system use three random functions f, g and h where random functions f and g map an m bit input string into an n-m bit string resembling a random number, and the random function h maps an n-m bit string into an m bit string resembling a random number. A random function maps inputs to outputs such that the outputs are unpredictable and random looking given the input. In the embodiments described below, the random functions are random oracles where every time an input is given it maps to the same output. Additionally, in the embodiments described below, the random functions are publicly known. For example, the random functions are known by the wireless communications system(s) involved in the intersystem handoff and the wireless unit.

[0024] The key conversion system is deterministic in that, given an m-bit key value, a wireless unit and the wireless communications system will determine the same n-bit key value without requiring an exchange of information. The key conversion system is reversible or bi-directional in that, if the wireless unit is handed off back to the first communications system, the n bit key of the second communications system is converted back to the m-bit key of the first communications system. The key conversion system provides improved security because even if almost all of the n bit key value is known, the m bit key value cannot easily be recovered. Similarly, if almost all of the m bit key value is known, the n bit key value is not easily recovered.

[0025] Depending on the embodiment, the key conversion system can provide secure, deterministic and bi-directional key conversion when a wireless unit roams between two wireless communications system, such as between an older communications system and a newer communications system. For example where the same reference numerals indicate like components, the IS-41 3G security scheme of FIG. 5 converts, at the VLR 80 and at the wireless unit 120 (or 122), the 520-bits VPM in combination with the 64-bits SMEKEY received from the VLR 110 to the 128-bit CK and/or 128-bit IK when the wireless unit roams into the 3G system from the 2G TDMA system. Conversely, as shown in FIG. 6, the IS-41 3G security scheme converts, at the VLR 80 and the wireless unit 90 (or 92), the 128-bit CK and/or the 128-bit IK to the 520-bits VPM in combination with the 64-bits SMEKEY when the wireless unit roams into the 2G TDMA system from the 3G system. The VLR 80

provides the VPM and the SMEKEY to the VLR 110.

[0026] As shown in FIG. 7, IS-41 3G security scheme converts, at the VLR 80 and at the wireless unit 120 (or 122), the 42-bits PLCM in combination with the 64-bits SMEKEY received from the VLR 110 to the 128-bit CK and/or the 128-bit IK when the wireless unit roams into the 3G system from the 2G CDMA system. Conversely, as shown in FIG. 8, the IS-41 3G security scheme converts, at the VLR 80 and at the wireless unit 90 (or 92), the 128-bit CK and 128-bit IK to the 42-bits PLCM in combination with the 64-bits SMEKEY when the mobile roams into the 2G CDMA system from the 3G system. The VLR 80 provides the PLCM and the SMEKEY to the VLR 110.

[0027] As shown in FIG. 9, the UMTS 3G security scheme converts, at the VLR 80 and at the wireless unit 60 (or 62), the 64-bit K_C received from the VLR 50 to the 128-bit CK and/or the 128-bit IK when the wireless unit roams into the 3G UMTS system from the 2G GSM system. Conversely, as shown in FIG. 10, the UMTS 3G security system converts, at the VLR 80 and at the wireless unit 90(or 92), the 128-bit CK and/or the 128-bit IK to the 64-bit K_C when the wireless unit roams into the 2G GSM system from the 3G UMTS system. The VLR 80 provides the K_C to the VLR 50.

[0028] Accordingly, in certain embodiments, a wireless unit that supports enhanced subscriber authentication (ESA) and enhanced subscriber privacy (ESP) in a first communications system, such as a newer 3G communications system, may implement multiple privacy modes to enable the wireless unit to provide privacy using older algorithms in a second communications system, such as an older 2G TDMA communications system. Such a wireless unit can provide other forms of privacy after intersystem handoff to an MSC for an older second communications system that does not support ESP. When handoff to the older second communications system is required, the key conversion system can convert the key values for the newer first communications system to the privacy keys needed for the older privacy algorithms supported by the older second communications system. The keys for the second communications system can be sent to the target MSC of the second communications system from the MSC of the first communications system. Since the key conversion system is deterministic, the wireless unit will also have the keys for the second communications system by performing the same conversion as the first communication system using the key conversion system of the present invention.

[0029] The key conversion system maps a key(s) from a first system into a key(s) of a second system and back again. For example, when performing an intersystem handoff between a 3G communications system and a 2G TDMA system, the key conversion system can map a cipher key CK into a VPMASK/SMEKEY (VS) pair. In this embodiment, the key conversion function possesses the following properties: 1) A 128 bit CK is mapped into a 584 bit VS; 2) The function is reversible and maps back a 584 bit VS into a 128 bit CK; and 3) The function is secure in the sense that partial knowledge of the 584 bit key will not allow the adversary to recover the CK, nor will partial knowledge of 128 bit key CK allow the adversary to recover the 584 bit VS. In certain instances, for example when the call originates in a first communication system having a larger key value than the target second communications system, the conversion system maps the key value of the first communication system to a key value of a second communications system. However, if the wireless unit returns to the first communications system, the key conversion system maps the second key value to a subsequent key value for the first communications system which is not necessarily the same as the original key value. Subsequent handoffs back to the first communications system from the second communications system produce a key value which is the same as the subsequent key value.

[0030] For example, when performing an intersystem handoff for a call originating with a 2G TDMA system to a 3G system, the key conversion system can map VPMASK/SMEKEY (VS) pair into a cipher key CK. In this embodiment, the key conversion function maps the 584 bit VS into the 128 bit CK. If the wireless unit is handed back to the 2G TDMA system, the conversion system maps back the 128 bit CK into the 584 bit VS, but the new 584 bit VS may not be the same as the original 584 bit VS. Subsequent handoffs to the 2G TDMA system from the 3G system will maintain the new 584 bit VS. Although this should not effect the security or operation of the wireless unit, the 128 bit CK is maintained the same all along in this embodiment.

[0031] In this embodiment, the key conversion system includes conversion functions available at the MSC in the newer system and at the wireless unit which will convert key values, for a first communications system, such as ESP keys, into key values of a second communications system, such as keys used for older privacy algorithms. In this example, the conversion function should convert the 128 bit CK key in the new first communication system to VPMASK/SMEKEY (VS) keys for the older second communication system. VPMASK is composed of 260 bits mask for each direction and SMEKEY is 64 bits long, for a total of 584 bits to be used by the older communication system. In case of an intersystem handoff from the old communication system to the new communication system, it may be useful for the conversion function to be reversible. The old communication system does not know about the new communication system and will transfer all 584 bits to the new communication system. The new communication system upon receiving the 584 bit key will realize that it needs to recover the 128 bit CK, and hence will compute the CK from the 584 bit key.

[0032] The VS keys created at the wireless unit and the MSC should be the same. This means the calculation of the VS keys must be based solely on CK and any

other quantities known by both the MSC and the wireless unit. Otherwise, any new quantities (e.g. random number) would have to be exchanged between the wireless unit and the MSC prior to the conversion. The key conversion system does not require the exchange of information between the wireless unit and the new MSC and deterministically maps a CK to VS keys and VS keys to a CK key.

[0033] Additionally, weaknesses in the old communications system should not make the new communications system weak. One can achieve this by making the key conversion function cryptographically one way, so that even if the entire key of the old communication system, such as the VS key in this example, is revealed, the adversary cannot recover the key of the new communication system, such as the CK key in this example. However, this will make the system non-reversible and, as previously noted, the key conversion system should be reversible. Nevertheless, the key conversion system can be reversible and still provide almost all of the security of a non-reversible function. The security of the key conversion system in this example prevents an adversary from recovering any part of the CK key even if almost all of the VS key is revealed except a small part. The adversary can guess the small part, but he should not be able to do any better. This aspect is important because parts of VPMASK may be somewhat easy to recover, and the entire VPMASK may be easier to recover than the SMEKEY. Yet if some part of the old system is hard to recover than the adversary will not know anything about CK. A similar security can apply to CK so that a partial knowledge of CK should not tell the adversary anything about VS.

[0034] In certain embodiments, the conversion function has two modes, the forward conversion and the reverse conversion. In the example of roaming from the 3G communications system to the 2G TDMA communications system, the forward conversion takes the 128 bit randomly created CK key and expands it to 584 bit VS key. The reverse conversion function takes the 584 bit VS keys and maps it to a 128 bit CK key. In this embodiment, the forward conversion function is composed of 3 random functions f, g and h which map a given input into a random output. In this embodiment, these are not secret functions but public random functions known to everybody, including the adversary. These public random functions are referred to as random oracles in the literature. These random oracles can be implemented using hash functions and block ciphers as described below. In this example, the three random functions are f, g, h where f and g map a 128 bit input into a 456 bit random value, and h maps a 456 bit input into a 128 bit random value.

[0035] FIG. 11 shows a flow diagram of an embodiment of the forward conversion of the key conversion system for converting an m-bit key value KEY1 of a first communications system into an n-bit key value KEY2 of a second communications system. The m bit KEY1 is provided to a random function f (block 200) which maps an m-bit string into an n-m bit random number or first intermediate value R. In the example of roaming from the 3G communications system to the 2G TDMA communications system, the conversion system converts a 128 bit key CK into a 584 bit key (VPMASK, SMEKEY). The 128 bit key CK is provided to the random function f (200) which maps the 128 bit CK into a 456 bit random number or first intermediate value R. The intermediate value R is provided to a random function h (block 210) which maps an n-m bit string into an m bit random number. The m-bit output of the function h (210) is subject to an exclusive-or (XOR 220) with the m bit KEY1 to produce an m-bit second intermediate value T. In the example of roaming from the 3G communications system to the 2G TDMA communications system, the 456 bit intermediate value R is provided to the function h (210). The function h (210) maps the 456 bit value R to a 128 bit random number which is XORed with the 128 bit CK to produce a 128 bit second intermediate value T.

[0036] In the embodiment of FIG. 11, the m-bit intermediate value T is provided to a random function g (block 230). The random function g (block 230) maps an m bit string to an n-m bit random number which is subject to an exclusive-or (XOR 240) with the n-m bit intermediate value R to produce an n-m bit key value V which can be used as a key, keys or portion(s) of key (s). In this embodiment, the value V is a portion of the value KEY2 which can be used as a key, keys or portion (s) of key(s). In this embodiment, the n bit key KEY2 includes the n-m bit value V along with the m bit second intermediate value T. In the example of roaming from the 3G communications system to the 2G TDMA communications system, the random function g (230) maps the 128 bit intermediate value T into a 456 bit random number which is subject to the exclusive-or (XOR 240) with the 456 bit intermediate value T to produce the 456 bit key value V. The 456 bit value V and the 128 bit intermediate value T form the 584 bit key value KEY2 which in this example can be divided into the VPMASK and the SMEKEY for 2G TDMA systems.

[0037] The forward conversion of the CK of the 3G system to the VPMASK and SMEKEY of the 2G TDMA system can be written according to the following steps.

1. R = f(CK) /* create a 456 bit value from 128 bit CK by applying f */
2. T = h(R) XOR CK /* create a 128 bit value using h */
3. V = g(T) XOR R /* create a 456 bit value using g */
4. Output T,V /* output the 584 bit value */

[0038] FIG. 12 shows a flow diagram of an embodiment of the reverse conversion of the key conversion system for converting the n-bit key value KEY2 of the second communications system back into the m-bit key value KEY1 of the first communications system. In this

embodiment, the n bit key value KEY2 is divided into an n-m bit first portion or value V and an m-bit second portion or value T. The m-bit value T is provided to the random function g (block 250) which maps an m-bit string into an n-m bit random number. The n-m bit random number is subjected to an exclusive-or (XOR 260) with the n-m bit key value V to produce the n-m bit first intermediate value R. In the example where the wireless unit roams back to the 2G TDMA system from the 3G system, the conversion system converts the 584 bit key (VPMASK, SMEKEY) into a 128 bit key CK. The 128 bit key value portion T is provided to the random function g (250) which maps the 128 bit T into a 456 bit random number. The 456 bit random number exclusive-ORed (XOR 260) with the 456 bit key value V to produce the 456 bit first intermediate value R.

[0039] In the embodiment of FIG. 12, the n-m bit first intermediate value R is provided to a random function h (block 270). The random function h (block 270) maps an n-m bit string to an m bit random number which is subject to an exclusive-or (XOR 280) with the m bit key value T to produce an m bit key value KEY1 which can be used as a key, keys or portion(s) of key(s). In the example where the wireless unit roams back to the 2G TDMA system from the 3G system, the random function h (270) maps the 456 bit intermediate value R into a 128 bit random number which is subject to an exclusive-or (XOR 280) with the 128 bit key value T to produce the 128 bit key CK.

[0040] The reverse conversion of the VPMASK and SMEKEY of the 2G TDMA system to the CK of the 3G system can be written according to the following steps.

1. Set T,V to 584 bit input /* T is 128 bit part, V is 456 bit part */
2. R = g(T) XOR V /* create 456 bit value R using T, V */
3. CK = h(R) XOR T

[0041] The random functions f, g and h can be implemented using hash functions and/or block ciphers. To implement the random functions f, g, and h, which can be referred to as random oracles, cyptographic hash functions, such as the functions known as known as SHA-1, MD5, RIPE-MD, can be used to instantiate the random functions f, g, h. A hash function can be typically characterized as a function which maps inputs of one length to outputs of another, and given an output, it is not feasible to determine the input that will map to the given output. Moreover, it is not feasible to find two inputs which will map to the same output. In using a SHA-1 hash function, each call to the SHA-1 hash function has a 160 bit initial vector (IV) and takes a 512 bit input or payload which is mapped into a 160 bit output. The IV is set to the IV defined in the standard for SHA-1 hash function. The payload will contain various input arguments: SHA(Type, Count, Input, Pad) where Type is a byte value which defines the various functions f, g, h. Function f and g will call SHA multiple times, and Count is a byte value which differentiates the multiple calls. Input is the input argument to the functions f, g, or h. Pad is zeroes to fill the remaining bit positions in the 512 bit SHA payload. Below is an example procedure for implementing the random function f, g and h using a hash function routine referred to as SHA.

SHA(type,count,input,pad)
f(CK): SHA(1, 1, CK, pad)
SHA(1, 2, CK, pad)
SHA(1, 3, CK, pad) mod 2^136
h(R): SHA(2, 1, R, pad) mod 2^128
g(T): SHA(3, 1, T, pad)
SHA(3, 2, T, pad)
SHA(3, 3, T, pad) mod 2^136

Block ciphers, like AES, can be used to create functions f, g, and h.

f(CK): $E_{CK}(1)$; $E_{CK}(2)$; $E_{CK}(3)$; $E_{CK}(4)$ mod 2^72;

h(R): E_{K0}(R1 XOR 5) XOR E_{K0}(R2 XOR 6) XOR E_{K0}(R3 XOR 7) XOR E_{K0}(R4 XOR 8)

g(T): $E_T(9)$; $E_T(10)$; $E_T(11)$; $E_T(12)$ mod 2^72;

where in f(CK), CK is used as the key in the block cipher and 512 bit stream is produced by encrypting 1...4 in counter mode. The last encryption is truncated from 128 bit to 72 bit to get the needed 456 bits. In h(R), a public key K0 is used to encrypt the parts of 456 bit R and the resulting ciphertexts are exclusive-ored together. R1, R2, and R3 are 128 bit values and R4 is the remaining 72 bit value of R, padded with zeroes to complete 128 bits.

[0042] Thus, the key conversion system provides bi-directional, deterministic and secure conversion of a key (s) or portion(s) thereof between first and second communications systems. The key conversion system is secure in the forward direction in that given most of the output KEY2 (for example, T,V), an adversary cannot recover KEY1 (for example, CK). In the example with the 2G TDMA and 3G systems, if all of T and most V except say 64 bits are known, then parts of R can be recovered, but not all of R by calculating R = g(T) XOR V. An attempt can be made to recover some of CK by performing CK = h(R) XOR T. However, since all of R is not known, even a bit of information about h(R) cannot be recovered, assuming h is a random function. Hence no information can be recovered about CK. Similarly, if all of V and part of T are known, except say 64 bits of T, then no information about CK can be recovered. Since we do not know all of T, the intermediate value R cannot be calculated using g(T) XOR V. Thus without the intermediate value R, no progress can be made in recovering any information about CK.

[0043] Similarly, the key conversion system is secure in the reverse direction in that given most of the output KEY1 (for example, CK), an adversary cannot recover KEY2 (for example, T, V). In the example with the 2G TDMA and 3G systems, if a part of CK is known, no information about T,V can be recovered. Since we do not

know all of CK, the intermediate value R cannot be calculated using f(CK). Thus without the intermediate value R, no progress can be made in recovering any information about T,V.

[0044] In addition to the embodiment(s) described above, the key conversion system according to the principles of the present invention can be used which omit and/or add input parameters and/or random functions or other operations and/or use variations or portions of the described system. For example, the key conversion system has been described as converting between n bit key of a first communication system and an m bit key of a second communications system using random oracles f, g and h where the random oracles f and g map an m bit string to a n-m bit random number and the random oracle h maps a n-m bit string to an m bit random number. However, different random functions can be used as well as different or additional functions which map x bit strings to y bit random numbers and/or map y bit strings to x bit random numbers where x or y can be equal to n-m or m. Additionally, the m bit key value for the first communications system can be a key, keys or portion(s) thereof, and the n bit key value for the second communications system can be a key, keys or portion (s) thereof. For example, the example with the 2G TDMA and 3G systems, the conversion is between the 128 bit CK of the 3G system and the 584 bit key value for the SMEKEY and VPMASK of the 2G TDMA system, but the conversion could be between a 256 bit key value of CK and IK of the 3G system and the 584 bit key value for the SMEKEY and VPMASK of the 2G TDMA system.

[0045] In the example described above, a forward conversion is from the m bit key value of the first communications system to the n bit key value of the second communications system where the first communications system corresponds to the new system and the second communications corresponds to the old system and where m<n. However, depending on the embodiment, the first communications system can be older, and the second communications system is newer. Alternatively, the forward conversion can be the conversion of the smaller size key value of one communications system to the larger bit size key value of another communications system, and the reverse conversion is the conversion of the larger bit size key value to the smaller size key value. Depending on the embodiment, the conversion of different, larger, smaller and/or the same size(s) of key value(s) between the different communications systems are possible.

[0046] Furthermore, the key conversion system can be used to handle the intersystem handoffs described in the FIGs 5-10 to convert a key, keys or portion(s) thereof from one communications system to the key, keys or portion(s) thereof of another communications system. It should be understood that different notations, references and characterizations of the various values, inputs and architecture blocks can be used. For example, the functionality described for the key conversion system can be performed in a home authentication center, home location register (HLR), a home MSC, a visiting authentication center, a visitor location register (VLR) and/or in a visiting MSC. Moreover, the key conversion system and portions thereof can be performed in a wireless unit, a base station, base station controller, MSC, VLR, HLR or other sub-system of the first and/or second communications system. It should be understood that the system and portions thereof and of the described architecture can be implemented in or integrated with processing circuitry in the unit or at different locations of the communications system, or in application specific integrated circuits, software-driven processing circuitry, programmable logic devices, firmware, hardware or other arrangements of discrete components as would be understood by one of ordinary skill in the art with the benefit of this disclosure. What has been described is merely illustrative of the application of the principles of the present invention. Those skilled in the art will readily recognize that these and various other modifications, arrangements and methods can be made to the present invention without strictly following the exemplary applications illustrated and described herein and without departing from the spirit and scope of the present invention.

Claims

1. A method of converting a first key value (key 1) for a first communications system to a second key value (key 2) of a second communications, said method **CHARACTERIZED BY**:

   generating a first intermediate value (R) from at least a portion of said first key value (key 1) using a first random function (f);
   providing at least a portion of said first intermediate value (R) to a second random function (h) to produce a second value;
   performing an exclusive-or (220) on at least a portion of said first key value (key 1) and at least a portion of said second value to generate a second intermediate value (T);
   providing at least a portion of said second intermediate value (T) to a third random function (g) to produce a third value; and
   producing at least a first portion of said second key value (key 2) by performing an exclusive-or (240) on at least a portion of said third value and at least a portion of said first intermediate value (R).

2. The method of claim 1 **CHARACTERIZED BY**:

   producing at least a portion of said second intermediate value (T) as at least a second portion of said second key value (key 2).

3. The method of claim 1 **CHARACTERIZED BY** said generating comprises the step of:

providing said first key value (key 1) of m bits to a first random function (f) to produce said first intermediate value (R) of n-m bits.

4. The method of claim 3 **CHARACTERIZED IN THAT** said first steps of providing and performing comprise:

providing said n-m bit first intermediate value (R) to a second random function (h) to produce an m bit second value; and
performing an exclusive-or (220) on said m bit first key value (key 1) and said m bit second value to generate said second intermediate value (T) with m bits.

5. The method of claim 4 **CHARACTERIZED IN THAT** said second step of providing and said step of producing comprise:

providing said m bit second intermediate value (T) to a third random function (g) to produce a n-m bit third value; and
performing an exclusive-or (240) on said n-m bit third value and said n-m bit first intermediate value (R) to generate an n-m bit portion (V) of said second key value (key 2).

6. The method of claim 5 **CHARACTERIZED BY**:

providing said m bit second intermediate value (T) as an m bit second portion of said second key value (key 2) having n bits.

7. The method of claim 2 **CHARACTERIZED BY** the steps of:

providing said second portion (T) of said second key value (key 2) to said third random function (g) to produce said third value; and
generating said first intermediate value (R) by subjecting said first portion (V) of said second key value (key 2) to an exclusive-or (260) with said third value.

8. The method of claim 7 further **CHARACTERIZED BY**:

using said second random function (h) to generate said second value from said first intermediate value (R); and
producing at least a portion of said first key by subjecting said second value to an exclusive-or (280) with said second portion (T) of said second key value (key 2).

9. A key conversion system for converting a first key value (key 1) for a first communications system to a second key value (key 2) of a second communications, said system **CHARACTERIZED BY**:

processing circuitry adapted to generate a first intermediate value (R) from at least a portion of said first key value (key 1) using a first random function (f) to provide at least a portion of said first intermediate value (R) to a second random function (h) to produce a second value, to perform an exclusive-or (220) on at least a portion of said first key value (key 1) and at least a portion of said second value to generate a second intermediate value (T), to provide at least a portion of said second intermediate value (T) to a third random function (g) to produce a third value and to produce at least a first portion of said second key value (key 2) by subjecting at least a portion of said third value to an exclusive-or (240) with at least a portion of said first intermediate value (R).

10. The system of claim 9 **CHARACTERIZED IN THAT** said processing circuitry further configured to produce at least a portion of said second intermediate value (T) as at least a second portion of said second key value (key 2).

FIG. 1

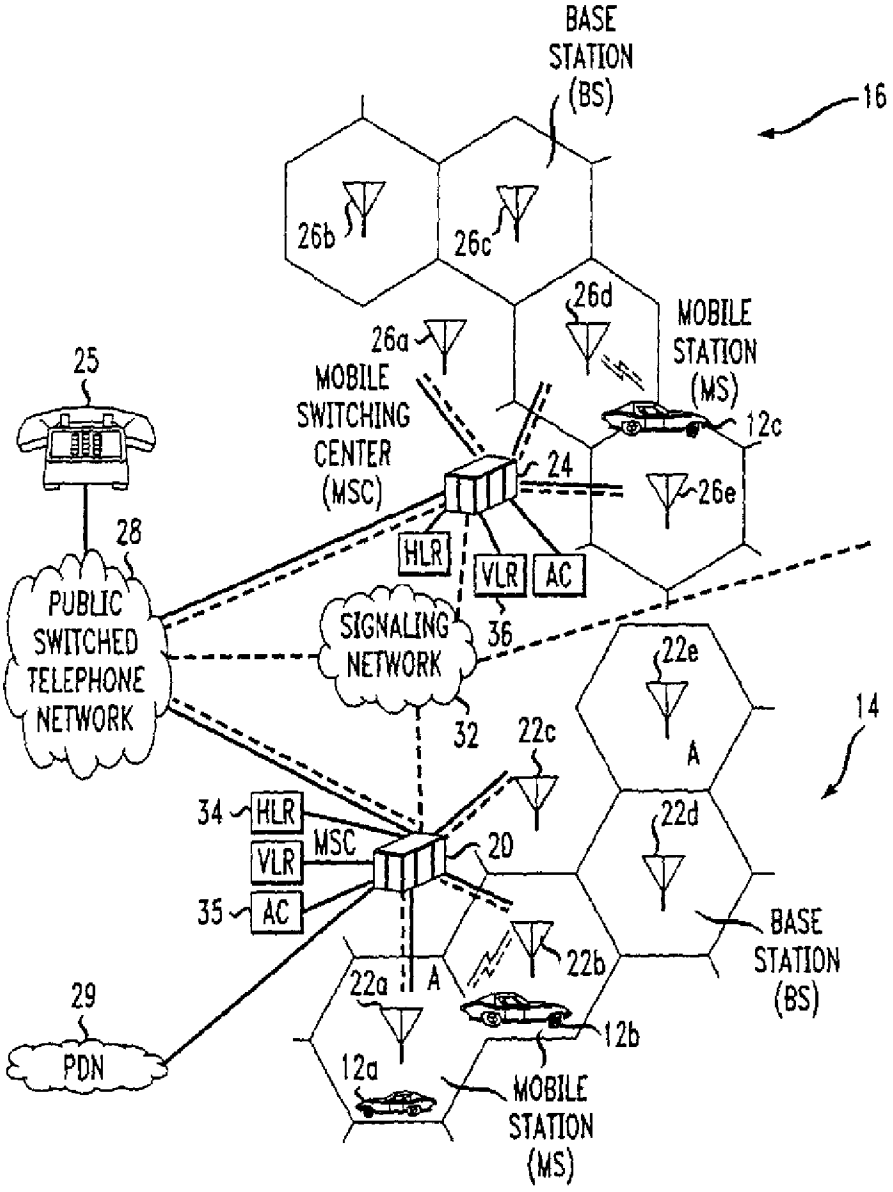

BASE STATION (BS)
16
26b
26c
26d
MOBILE STATION (MS)
12c
26a
MOBILE SWITCHING CENTER (MSC)
25
24
26e
28
HLR
VLR
AC
PUBLIC SWITCHED TELEPHONE NETWORK
SIGNALING NETWORK
36
32
22e
A
14
22c
22d
34
HLR
VLR
35
AC
MSC
20
BASE STATION (BS)
22a
A
22b
12b
29
PDN
12a
MOBILE STATION (MS)

FIG. 2

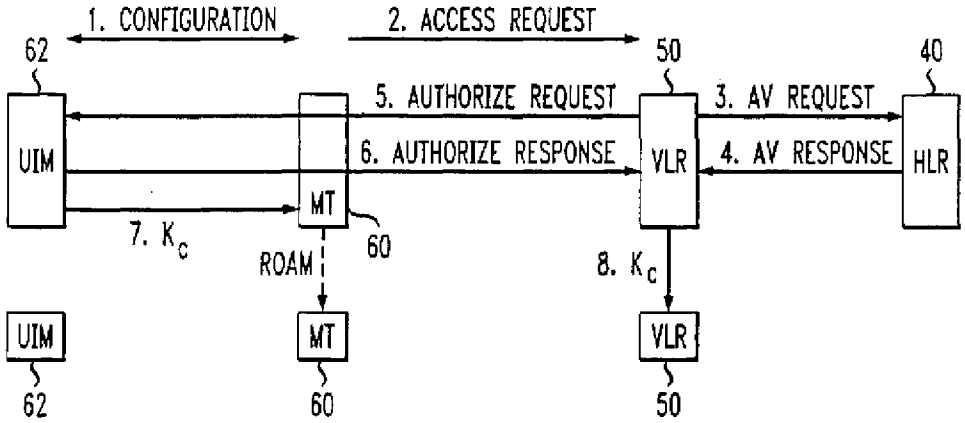

1. CONFIGURATION
2. ACCESS REQUEST
62
50
40
5. AUTHORIZE REQUEST
3. AV REQUEST
UIM
6. AUTHORIZE RESPONSE
VLR
4. AV RESPONSE
HLR
MT
7. K_c
60
ROAM
8. K_c
UIM
MT
VLR
62
60
50

FIG. 3

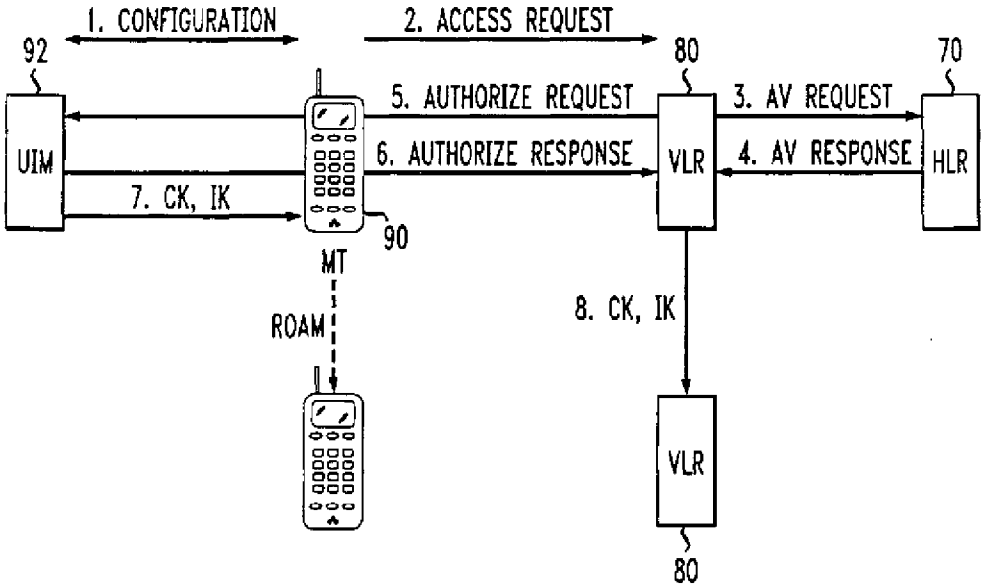

1. CONFIGURATION
2. ACCESS REQUEST
92
80
70
5. AUTHORIZE REQUEST
3. AV REQUEST
UIM
6. AUTHORIZE RESPONSE
VLR
4. AV RESPONSE
HLR
7. CK, IK
90
MT
ROAM
8. CK, IK
VLR
80

FIG. 4

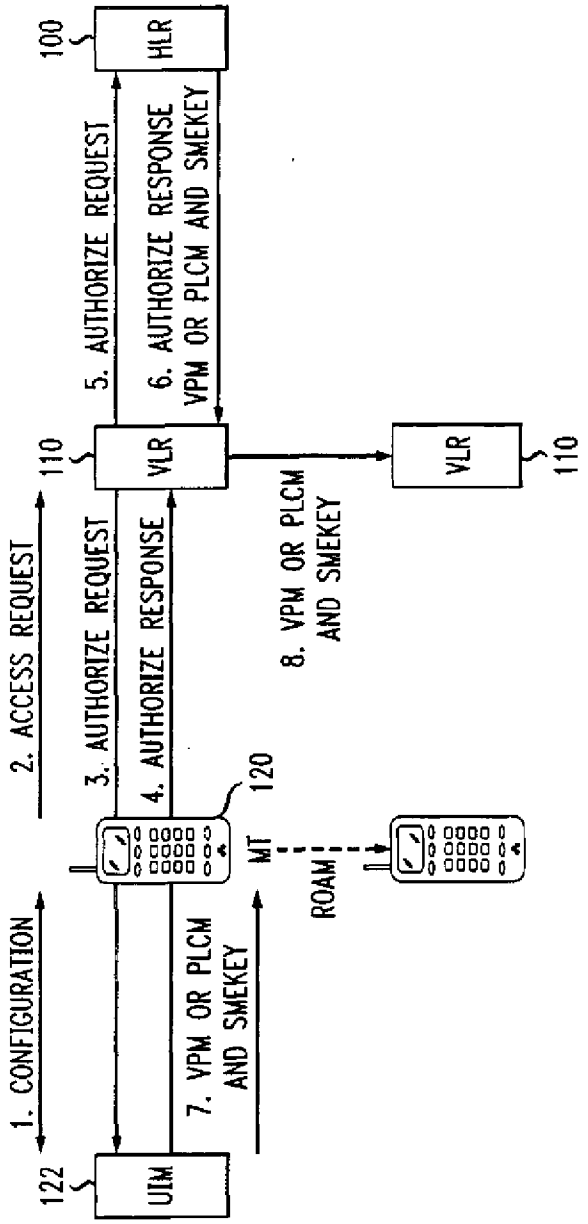

100
HLR
5. AUTHORIZE REQUEST
6. AUTHORIZE RESPONSE
VPM OR PLCM AND SMEKEY
110
VLR
2. ACCESS REQUEST
3. AUTHORIZE REQUEST
4. AUTHORIZE RESPONSE
8. VPM OR PLCM
AND SMEKEY
VLR
110
120
MT
ROAM
1. CONFIGURATION
7. VPM OR PLCM
AND SMEKEY
122
UIM

FIG. 5

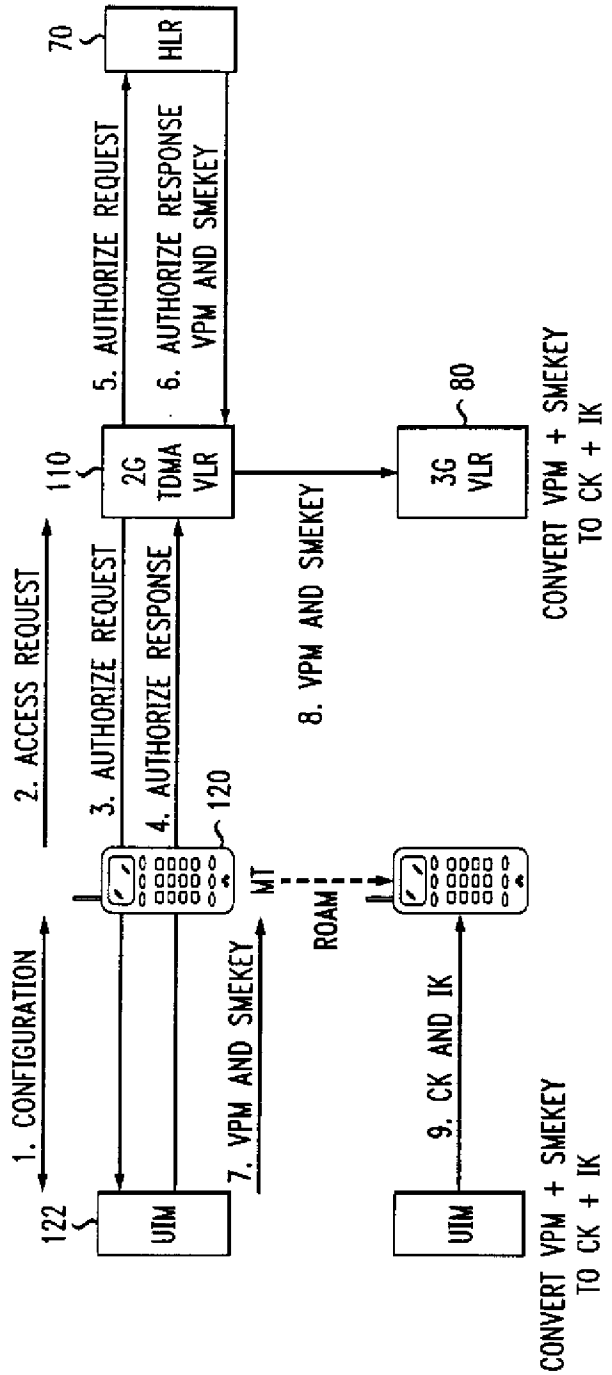

70
HLR
5. AUTHORIZE REQUEST
6. AUTHORIZE RESPONSE
VPM AND SMEKEY
110
2G
TDMA
VLR
80
3G
VLR
2. ACCESS REQUEST
3. AUTHORIZE REQUEST
4. AUTHORIZE RESPONSE
8. VPM AND SMEKEY
CONVERT VPM + SMEKEY
TO CK + IK
120
1. CONFIGURATION
MT
ROAM
7. VPM AND SMEKEY
9. CK AND IK
122
UIM
UIM
CONVERT VPM + SMEKEY
TO CK + IK

FIG. 6

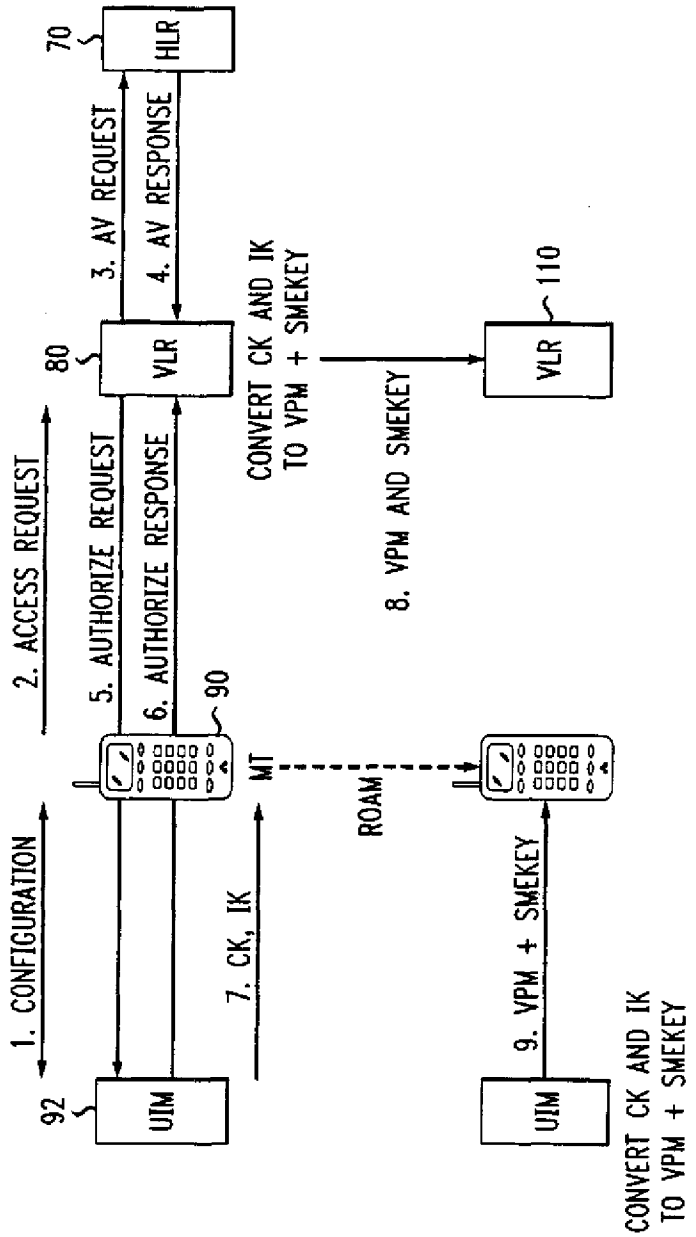

70
HLR
3. AV REQUEST
4. AV RESPONSE
80
VLR
2. ACCESS REQUEST
5. AUTHORIZE REQUEST
6. AUTHORIZE RESPONSE
CONVERT CK AND IK
TO VPM + SMEKEY
8. VPM AND SMEKEY
110
VLR
90
MT
ROAM
1. CONFIGURATION
7. CK, IK
9. VPM + SMEKEY
92
UIM
UIM
CONVERT CK AND IK
TO VPM + SMEKEY

FIG. 7

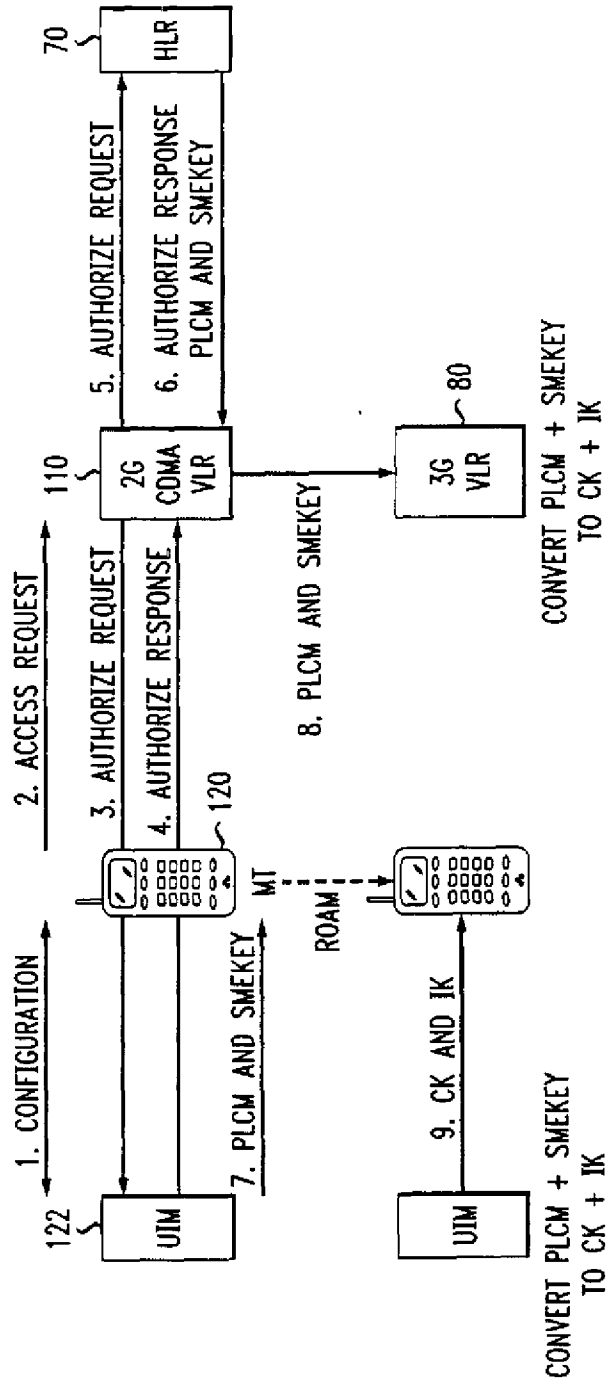

70
HLR
5. AUTHORIZE REQUEST
6. AUTHORIZE RESPONSE
PLCM AND SMEKEY
110
2G
CDMA
VLR
2. ACCESS REQUEST
3. AUTHORIZE REQUEST
4. AUTHORIZE RESPONSE
120
8. PLCM AND SMEKEY
80
3G
VLR
CONVERT PLCM + SMEKEY
TO CK + IK
1. CONFIGURATION
122
UIM
7. PLCM AND SMEKEY
MT
ROAM
9. CK AND IK
UIM
CONVERT PLCM + SMEKEY
TO CK + IK

FIG. 8

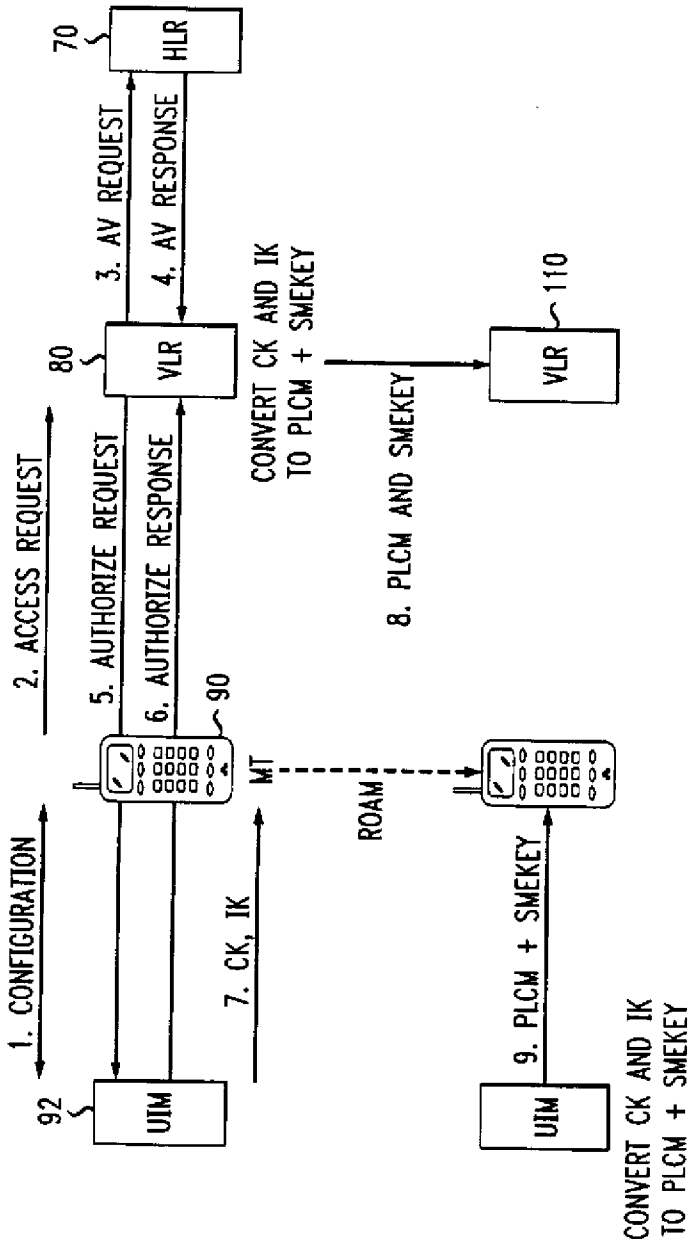

70
HLR
3. AV REQUEST
4. AV RESPONSE
80
VLR
2. ACCESS REQUEST
5. AUTHORIZE REQUEST
6. AUTHORIZE RESPONSE
90
CONVERT CK AND IK
TO PLCM + SMEKEY
8. PLCM AND SMEKEY
110
VLR
1. CONFIGURATION
92
UIM
7. CK, IK
MT
ROAM
9. PLCM + SMEKEY
UIM
CONVERT CK AND IK
TO PLCM + SMEKEY

FIG. 9

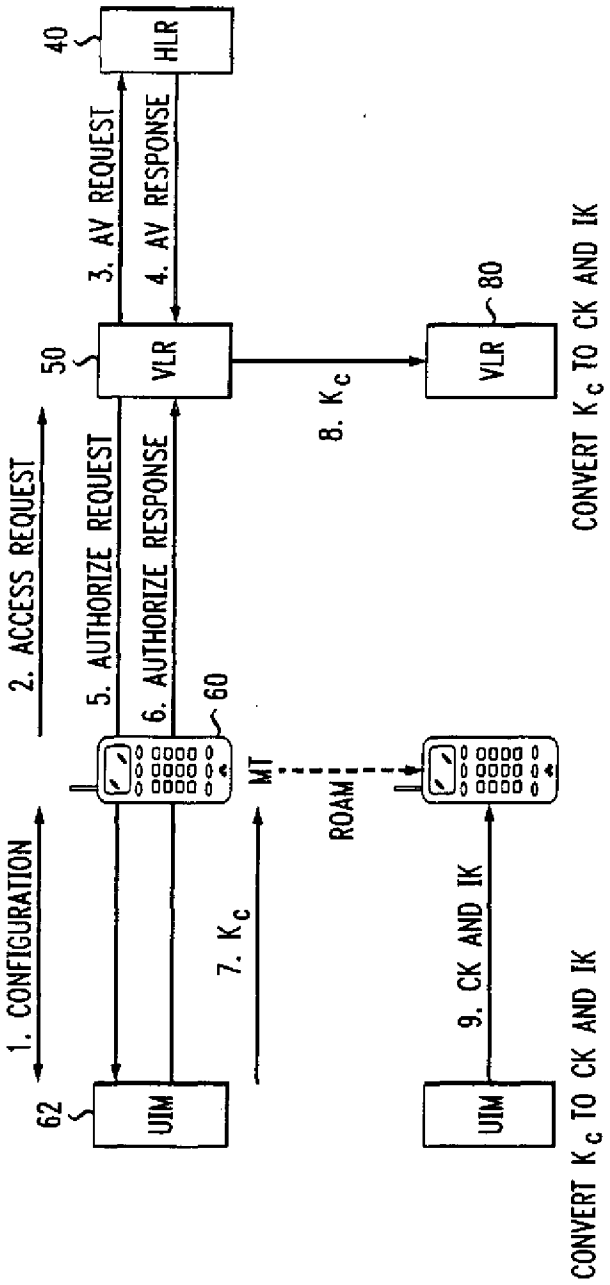

40
HLR
3. AV REQUEST
4. AV RESPONSE
50
VLR
8. K_c
80
VLR
CONVERT K_c TO CK AND IK
2. ACCESS REQUEST
5. AUTHORIZE REQUEST
6. AUTHORIZE RESPONSE
60
MT
ROAM
1. CONFIGURATION
7. K_c
9. CK AND IK
62
UIM
UIM
CONVERT K_c TO CK AND IK

FIG. 10

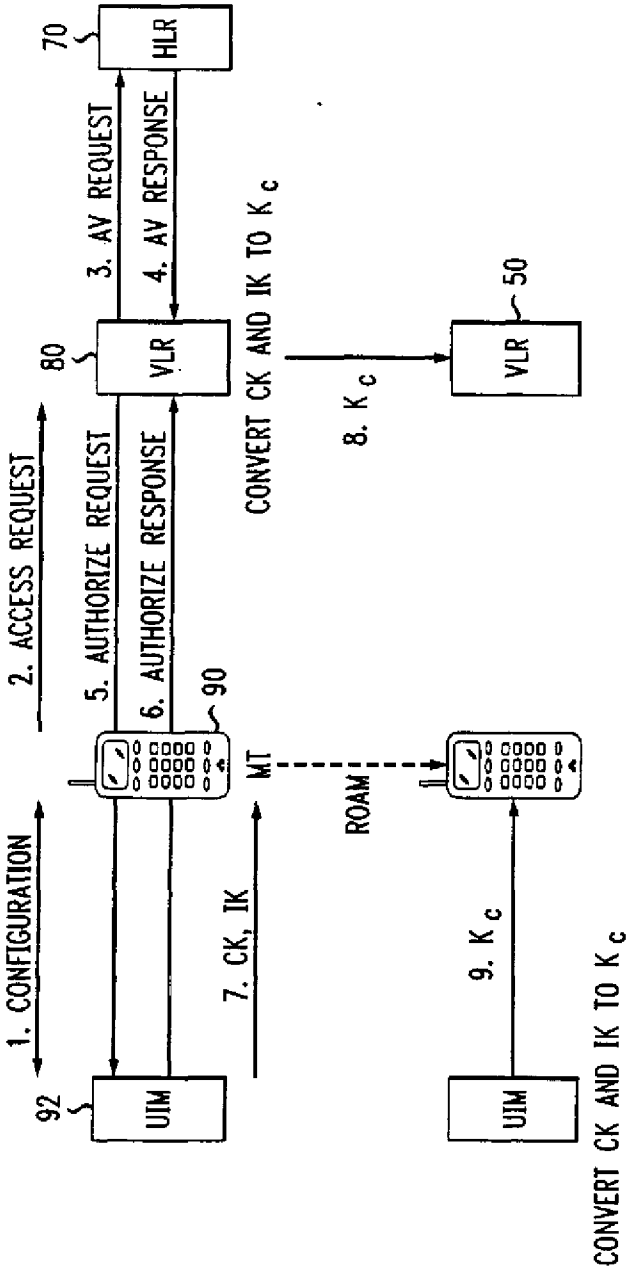

70
HLR
3. AV REQUEST
4. AV RESPONSE
80
VLR
2. ACCESS REQUEST
5. AUTHORIZE REQUEST
6. AUTHORIZE RESPONSE
90
CONVERT CK AND IK TO Kc
8. Kc
50
VLR
1. CONFIGURATION
92
UIM
7. CK, IK
MT
ROAM
9. Kc
UIM
CONVERT CK AND IK TO Kc

FIG. 11

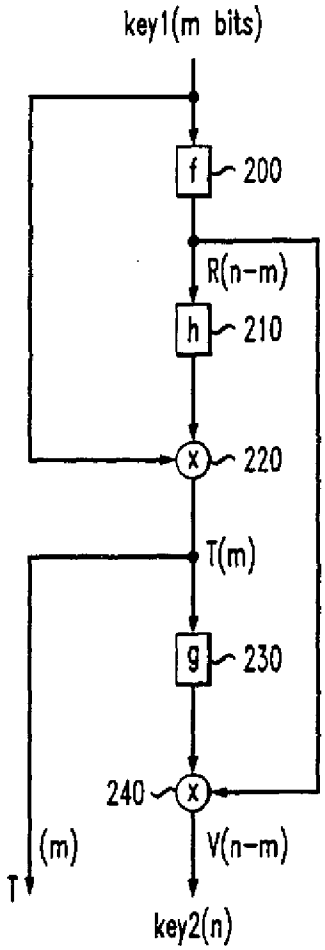
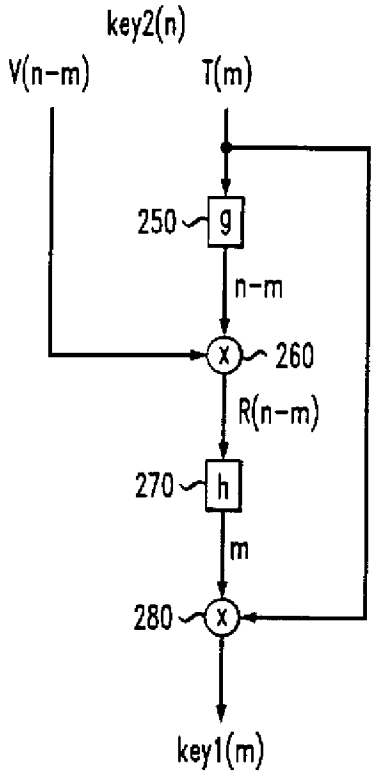


FIG. 12



European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 01 30 6907

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
A	MENEZES: "Handbook of applied cryptography" 1997 , CRC PRESS LLC , US XP002191213 * page 331, line 5 - line 9 * * page 568, line 14 - line 35 *	1-10	H04Q7/38
P,A	WO 00 76194 A (NOKIA NETWORKS OY ;EINOLA HEIKKI (FI); EKOLA KEIJO (FI); LINDHOLM) 14 December 2000 (2000-12-14) * abstract *	1-10	
A	US 5 594 795 A (DENT PAUL W ET AL) 14 January 1997 (1997-01-14) * abstract *	1-10	

TECHNICAL FIELDS SEARCHED (Int.Cl.7)

H04L
H04Q

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
BERLIN	7 March 2002	San Millán Maeso, J

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 01 30 6907

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on. The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

07-03-2002

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0076194 A	14-12-2000	FI 991283 A	05-12-2000
		AU 5223400 A	28-12-2000
		EP 1103137 A1	30-05-2001
		WO 0076194 A1	14-12-2000
US 5594795 A	14-01-1997	AU 692288 B2	04-06-1998
		AU 3092095 A	25-01-1996
		BR 9508228 A	28-10-1997
		DE 69518521 D1	28-09-2000
		DE 69518521 T2	11-01-2001
		EP 0769237 A1	23-04-1997
		FI 970046 A	07-01-1997
		JP 10502507 T	03-03-1998
		NZ 290238 A	26-06-1998
		WO 9601546 A1	18-01-1996

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 248 188 A1

(12) EUROPEAN PATENT APPLICATION

published in accordance with Art. 158(3) EPC

(43) Date of publication:
09.10.2002 Bulletin 2002/41

(21) Application number: **02710388.6**

(22) Date of filing: **30.01.2002**

(51) Int Cl.7: **G06F 9/06**, G06F 9/445

(86) International application number:
PCT/JP02/00699

(87) International publication number:
WO 02/061572 (08.08.2002 Gazette 2002/32)

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR

(30) Priority: **31.01.2001 JP 2001024738**
22.03.2001 JP 2001083567

(71) Applicant: **NTT DoCoMo, Inc.**
Tokyo 100-6150 (JP)

(72) Inventors:
- **NATSUNO, Takeshi**
Meguro-ku, Tokyo 153-0062 (JP)
- **ITAGAKI, Takatoshi**
Edogawa-ku, Tokyo 134-0084 (JP)
- **MORIGUCHI, Atsushi**
Bunkyou-ku, Tokyo 113-0033 (JP)

(74) Representative: **HOFFMANN EITLE**
Patent- und Rechtsanwälte
Arabellastrasse 4
81925 München (DE)

(54) SYSTEM FOR DELIVERING PROGRAM TO STORAGE MODULE OF MOBILE TERMINAL

(57) A UIM 12 having a plurality of storage areas is built into or mounted in a mobile terminal 11. A contents server 19, upon receipt of a distribution request from the mobile terminal 11, distributes a program or data used at the time of program execution or the program itself through a network including a radio network. This program and the data or the program itself are stored in the storage area of the UIM 12 and not through the control unit of the mobile terminal 11.

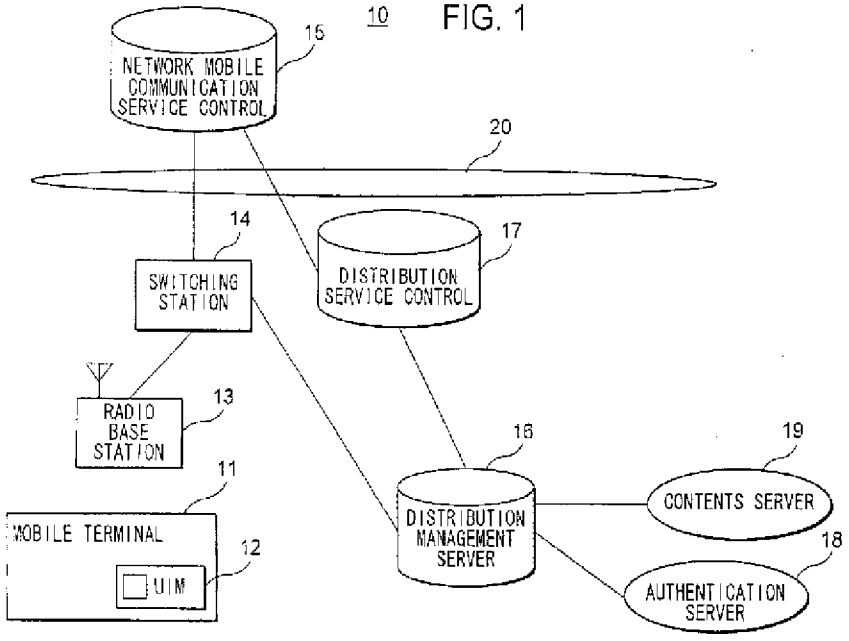


FIG. 1

EP 1 248 188 A1

Description

TECHNICAL FIELD

[0001] The present invention relates to a technique for distributing a program (application or applet) to a storage module built or mounted in a mobile terminal.

BACKGROUND ART

[0002] In recent years, a mobile terminal has been developed which has a program executing environment. An example of a mobile terminal of this type is one which has a Java virtual machine. The user installs a program in the mobile terminal and thus can add a desired function to the mobile terminal.

[0003] However, even if desirable functions are added to a mobile terminal, a user is liable to become tired of using the same mobile terminal after a protracted period. On the other hand, the mobile terminal industry suffers fierce competition and various new products, attractive to users, have been successively placed on the market. A user may want to change his mobile terminal with a new desirable product placed on the market. Once the mobile terminal is replaced, however, the functions that have hitherto been added to the old mobile terminal cannot be used any longer. If the same functions are to be used even after the change of a mobile terminal, the programs that have been installed in the old mobile terminal have to be installed in the new mobile terminal. This is a troublesome job.

DISCLOSURE OF THE INVENTION

[0004] This invention has been achieved in view of the situation described above, and the object thereof is to provide a system in which even after a mobile terminal is changed, the programs that could be used before the change of the mobile terminal, can be continuously used after the change.

[0005] In order to achieve this object, the present inventors have taken notice of a certain type of a mobile terminal, that is to say, a mobile terminal capable of being mounted or having fitted therein a module for storing the subscriber information including the subscriber number and the memory dial information (hereinafter referred to as the user ID module or UIM). The user of this type of the mobile terminal, whenever desirous of changing it with a new mobile terminal, can use the new mobile terminal in similar manner simply by mounting or building into the new mobile terminal the UIM which he may have. In connection with this, the present inventors have come up with the following idea. Specifically, once a program is stored in this UIM, the program used with the old mobile terminal can be easily transferred to the new mobile terminal for an improved operating convenience of the user.

[0006] Nevertheless, the problem of security has been an obstacle to realizing such a novel mobile terminal.

[0007] First, as long as no limit is set on the operation of writing a program in the UIM, the inherent functions of the mobile terminal may be undesirably destroyed intentionally or negligently.

[0008] Also, the subscriber information stored in the UIM may include the personal information or data having monetary value. From the viewpoint of security, therefore, careful consideration is necessary not to cause the leakage of this information in writing a program in the UIM.

[0009] In order to solve this security problem and improve the operating convenience for the user, according to the present invention, there is provided a program distribution system comprising a mobile terminal having means for transmitting a program distribution request, a storage module built in or connected to the mobile terminal, a contents server for receiving the distribution request and transmitting a program to be distributed, and a distribution management server for receiving the program from the contents server and, as long as the contents server is authorized, transmitting the program received from the contents server to the storage module built in or connected to the mobile terminal, characterized in that the storage module includes a storage unit, and a control unit for storing in the storage unit the program received from the distribution management server through the mobile terminal and executing the program stored in the storage unit in response to a request.

[0010] Also, according to the present invention, there is provided a program distribution system comprising a mobile terminal having means for transmitting a program distribution request, a storage module built in or connected to the mobile terminal, and a distribution management server for receiving the distribution request; and in the case where the program to be distributed is provided by the authorized contents server, acquiring and transmitting the program to the storage module built in or connected to the mobile terminal, characterized in that the storage module includes a storage unit, and a control unit for receiving the information through the mobile terminal, storing the information in the storage unit only in the case where the information is the program received from the distribution management server and executing the program stored in the storage unit in response to a request.

[0011] With these systems, only a program supplied through the distribution management server from an authorized contents server is written in the storage module and therefore, the user can write a new program in the storage module with guaranteed security.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012]

Fig. 1 is a block diagram showing a configuration of

a program distribution system according to a first embodiment of the invention.

Fig. 2 shows the external appearance of a mobile terminal according to the same embodiment.

Fig. 3 is a block diagram showing a configuration of the same mobile terminal.

Fig. 4 is a diagram showing a configuration of the same mobile terminal and the UIM built in or connected to it.

Fig. 5 is a sequence diagram showing the process from program distribution to activation according to the same embodiment.

Fig. 6 is a sequence diagram showing the program distribution operation according to the same embodiment.

Fig. 7 is a diagram showing a display screen of the mobile terminal at the time of program distribution.

Fig. 8 is a sequence diagram showing the program activation operation according to the same embodiment.

Fig. 9 is a sequence diagram showing the processes of the program deactivation in compliance with a request from the contents server according to the same embodiment.

Fig. 10 is a sequence diagram showing the process of the program delete operation in compliance with a request from the contents server according to the same embodiment.

Fig. 11 is a sequence diagram showing the process of the program deactivate operation and the program delete operation in compliance with a request from the distribution management server according to the same embodiment.

Fig. 12 is a sequence diagram of the UIM exchanging the version information according to the same embodiment.

Fig. 13 is a sequence diagram showing the process ending in a program distribution failure due to a memory shortage.

Fig. 14 is a sequence diagram showing the process ending in a program distribution failure due to a memory error.

Fig. 15 is a diagram showing a display screen provided to the user at the time of program deletion.

Fig. 16 is a diagram showing a display screen provided to the user at the time of account settlement for an electronic commercial transaction.

Fig. 17 is a diagram showing a display screen provided to the user at the time of commodity purchase in male order sale.

Fig. 18 is a diagram showing a display screen for setting the automatic program start.

Figs. 19 and 20 are diagrams showing a display screen at the time of using a commutation pass.

Fig. 21 is a block diagram showing a configuration of a program distribution system according to a second embodiment of the invention.

Fig. 22 is a diagram showing a configuration of a memory in the UIM according to the same embodiment.

Fig. 23 is a block diagram showing a configuration of a distribution management server 16A according to the same embodiment.

Fig. 24 is a sequence diagram showing the process for registration in a user information storage unit.

Figs. 25 and 26 are sequence diagrams showing the operation of registering a program registered in the user information storage unit, in any of the basic blocks of the UIM 12.

Figs. 27 and 28 are sequence diagrams showing the operation of registering a program registered in the user information storage unit, in any of the basic blocks of the UIM.

Fig. 29 is a sequence diagram showing the operation of deleting a program registered in the user information storage unit 51.

Fig. 30 is a sequence diagram showing the operation of deleting a program registered in the basic blocks of the UIM.

Fig. 31 is a sequence diagram showing the deactivation process for the user information storage unit.

Fig. 32 is a sequence diagram showing the deactivation process for the basic blocks.

BEST MODE FOR CARRYING OUT THE INVENTION

[0013] Now, preferred embodiments of the invention will be explained with reference to the drawings.

[1] First embodiment

[1.1] General configuration of program distribution system

[0014] Fig. 1 is a block diagram showing a configuration of a program distribution system according to a first embodiment of the invention.

[0015] A program distribution system 10 roughly comprises a mobile terminal 11, a radio base station 13, a switching station 14, a network mobile communication service control unit 15, a distribution management server 16, a distribution service control unit 17, an authentication server 18, a contents server 19 and a public network 20.

[0016] The mobile terminal 11 is an information processing unit, for example, having communication functions such as a portable telephone or a PHS (Personal Handyphone System (registered trade name)). Further, the mobile terminal 11 has mounted or built therein a UIM (User Identification Module) 12 capable of storing various programs or data.

[0017] The radio base station 13 communicates with the mobile terminal 11 through a radio link.

[0018] The switching station 14 controls the switching operation between the mobile terminal 11 and a common channel interoffice signal network 20 constituting a

wire network, connected to each other through the radio base station 13.

[0019] The network mobile communication service control unit 15 controls the communication in the case where a program is distributed to the mobile terminal 11 through the public network 20.

[0020] The contents server 19 distributes various contents on the one hand and distributes a program as requested from the mobile terminal 11 on the other.

[0021] The distribution management server 16 relays and manages the distribution of a program from the contents server 19 to the UIM 12. The distribution of a program to the UIM 12 and access to a program stored in the UIM 12 are carried out always through the distribution management server 16. This is the most significant feature of this embodiment.

[0022] The distribution service control unit 17 operates like an interface between the distribution management server 16 and the public network 20 in the case where a program is distributed through the public network 20.

[0023] The authentication server 18 is a device for issuing a certificate required for program distribution to the contents server 19. This certificate includes a UIM public key having the function of explaining, for the benefit of the UIM 12, that the contents server 19 is duly authorized to distribute a program to the UIM 12, and a distribution management server public key having the function of certifying, for the benefit of the distribution management server 16, that the contents server 19 is similarly authorized.

[0024] The contents server 19, the distribution management server 16 and the authentication server 18 according to this embodiment have the following functions, respectively.

(a) According to this embodiment, the contents server 19 sends a program addressed to the UIM 12, to the distribution management server 16, which in turn distributes the program to the UIM 12. The contents server 19 never distributes the program directly to the UIM 12.

(b) The contents server 19 distributes a program to the UIM 12 by encrypted communication of a public-key type with the distribution management server 16 as an intermediary. The UIM 12 of each user is equipped with a PKI (public key infrastructure), and each UIM 12 has a UIM private key unique to the particular UIM 12. For distributing a program addressed to a given UIM 12, the contents server 19 acquires a UIM public key paired with a UIM private key for the particular UIM 12, whereby the program is encrypted.

(c) According to this invention, only an authorized contents server 19 can distribute a program addressed to the UIM 12. The authorized contents server 19 is assigned a distribution management server public key. The contents server 19, upon receipt of a distribution request from the mobile terminal 11, further encrypts, by the distribution management server public key, the program already encrypted by the UIM public key and addressed to the UIM 12, and sends it to the distribution management server 16.

[1.2] Configuration of mobile terminal

[0025] Fig. 2 shows the external appearance of the mobile terminal 11. The mobile terminal 11 includes a display section 21 and an operating section 22.

[0026] As shown in Fig. 2, various processing menu items, the screen being browsed, the telephone number screen, etc. are displayed on the display section 21.

[0027] The operating section 22 has a plurality of operating buttons for inputting various data and displaying menu item screens. One of the operating buttons of the operating unit 22 is a UIM button 23. The UIM button 23 is operated by the user for utilizing a program stored in the UIM 12.

[0028] Fig. 3 is a block diagram showing a configuration of a mobile terminal.

[0029] The mobile terminal 11 includes a display section 21, an operating section 22, a control unit 31, a storage unit 32, an external equipment interface (I/F) unit 33, a communication unit 34, a UIM interface (I/F) unit 35 and an voice input/output unit 36.

[0030] The control unit 31 controls the various parts of the mobile terminal 11 based on the control data and the control program stored in the storage unit 32.

[0031] The storage unit 32 is configured of a ROM, a RAM, etc., and has a plurality of storage areas including a program storage area for storing various programs such as a browser for accessing an internet and a data storage area for storing various data.

[0032] The external equipment I/F unit 33 is an interface utilized by the control unit 31 and the UIM 12 for exchanging information with an external device.

[0033] The communication unit 34 transmits various data including audio and text messages to the radio base station 13 through the antenna 34A under the control of the control unit 31 on the one hand, and receives various data sent to the mobile terminal 11 through the antenna 34A on the other hand.

[0034] The UIM I/F unit 35 inputs/outputs data from and to the control unit 31. The UIM I/F unit 35 also outputs the output data from the communication unit 34 or the external equipment I/F unit 33 to the UIM 12 without the intermediation of the control unit 31. Also, the output data of the UIM 12 is output directly to the external equipment I/F unit 33 or the communication unit 34 directly without the intermediation of the control unit 31. The reason why the data are input/output from and to the external equipment I/F 33 or the communication unit 34 without the intermediation of the control unit 31, is in order to prevent an illegal access to the data on the UIM 12 by the alteration of the control program of the control

unit 31 and thus to maintain security.

[1.3] Configuration of UIM

[0035] Fig. 4 shows a configuration of the UIM 12. In Fig. 4, a part of the component elements of the mobile terminal 11 are shown together with the component elements of the UIM 12 to clarify the relation with the mobile terminal 11. As shown in Fig. 4, the UIM 12 includes a memory 12M, which in turn, roughly, has a system area 12A and an application area 12B.

[0036] The system area 12A has stored therein personal information data unique to each user such as subscriber number data, outgoing call history information data, incoming call history information data, speech time information data and a UIM private key. The mobile terminal 11 communicates with other communication units using the subscriber number data in the system area 12A as a calling line identity.

[0037] The application area 12B is for storing the program distributed and the data used at the time of execution of the program, and divided into a plurality of basic blocks. In the case shown in Fig. 4, the application area 12B is divided into six basic blocks 40-1 to 40-6.

[0038] The basic blocks 40-1 to 40-6 each include a program area 41 and a data area 42. The program area 41 of each basic block 40-k has stored therein a program (an application or an applet). The data area 42 of each basic block 40-k, on the other hand, has stored therein the data used at the time of executing the program in the program area 41 of the same basic block 40-k.

[0039] The basic blocks 40-1 to 40-6 are independent of each other, and are basically so managed that the application or the applet stored in the program area 41 of a given basic block 40-j cannot access the data area 42 of another basic block 40-k ($\neq$ j). By employing this configuration, the security of each program is maintained. Even in the case where data having a monetary value (what is called "a value") are recorded in the data area 42 of a given basic block 40-j, therefore, the particular data is never rewritten, intentionally or incidentally, by a program stored in another basic block 40-k ($\neq$ j).

[0040] The application or the applet constituting a program stored in the program area 41, on the other hand, cannot be distributed or deleted without the intermediary of the distribution management server 16. The data area 42, however, can be operated directly through the distribution management server 16 or a local terminal as in the case where the electronic money is downloaded from an ATM.

[0041] Further, the application area 12 has a storage area for an activation flag indicating whether the program in the program area 41 of each of the basic blocks 40-1 to 40-6 can be executed or not.

[0042] The control unit 30 is a means for writing a program for the basic block of the application area 12B, setting or resetting the activation flag corresponding to each basic block or executing a program in a designated basic block, in response to a request given through the mobile terminal 11. Upon arrival of a program encrypted by the UIM public key from the distribution management server 16, the control unit 30 decrypts the program using the UIM private key in the system area 12 and writes it in a basic block. Also, the control unit 30 can execute the program in the basic block. In the process, the information required by the program in execution is acquired from the other party of the communication in the network or from the user of the mobile terminal 11 through the browser executed by the mobile terminal 11. The control unit 30 can also send the result of program execution to the other party of communication in the network or send it to the user of the mobile terminal 11 through the browser. Also, the control unit 30 can exchange information with external devices through the hardware resources of the mobile terminal 11 without the intermediary of the browser in accordance with the program in the basic block. An example of a program available for this purpose is an application program for causing the mobile terminal 11 to function as a commutation pass. In executing this program, the control unit 30 can exchange the pass information with the card reader/writer at the gates of a railway station utilizing a short-range radio unit (not shown) connected to the external equipment I/F of the mobile terminal 30. The program for the control unit 30 to perform the various processes described above, including the execution and control of the program in the application area is stored in the system area 12A.

[1.4] Operation of first embodiment

[0043] Now, the operation of the first embodiment will be explained taking the distribution of the commutation pass applet as an example.

[0044] Fig. 5 is a sequence diagram showing the process of program distribution, write operation and activation.

[0045] As shown in Fig. 5, these series of processes are roughly configured of the step of distributing an inactive program (applet) as a memory module to the UIM 12 and writing it in the UIM 12 (step S1), and an activation step for activating the program written (step S2).

[1.4.1] Issue of certificate to distribution management server

[0046] Fig. 6 is a sequence diagram showing the process of distributing a program and writing it in the UIM 12. As shown in Fig. 6, the authentication server 18 issues a certificate to the contents server 19 permitted to distribute the program addressed to the UIM 12 (step S11). The certificate is issued to enable the contents server 19 and the distribution management server 16 to perform the encryption communication based on the public key encryption method. Specifically, in order to make possible the encryption communication using a

public key, a distribution management server private key and a distribution management server public key, constituting a pair, are generated. The distribution management server private key is stored in the distribution management server 16, while the distribution management server public key is transmitted from the authentication server 18 to the contents server 19 as a certificate identifying a person permitted to distribute a program. The contents server 19, upon receipt of the distribution management server public key, stores it in preparation for program distribution.

[1.4.2] Program distribution request

[0047] The user can cause the control unit 31 to execute the browser and thus can access the home page of the contents provider by operating the operating section 22 of the mobile terminal 11. As a result of this access, a distribution menu screen D1 indicating the program distribution performed by the contents server 19 of the contents provider is displayed, as shown in Fig. 7, on the display section 21 of the mobile terminal 11. Under this condition, the user transmits a program (applet) distribution request from the mobile terminal 11 through the network to the contents server 19 by operating the operating section 22 of the mobile terminal 11 (step S12).

[1.4.3] Certificate issue request to UIM

[0048] The contents server 19, upon receipt of a distribution request from the mobile terminal 11, sends a certificate issue request to the authentication server 18 (step S12). This certificate issue request contains the information for specifying the UIM 12 of the mobile terminal 11. The certificate issue is requested in order to enable the contents server 19 to conduct the encryption communication of public key type with the UIM 12. More specifically, in order to make possible the encryption communication of public key type, the UIM private key and the UIM public key paired with the former are generated in advance, and the UIM private key is stored in the UIM 12 in advance, while the UIM public key is stored in the authentication server 18 in advance. In step S12, the UIM public key stored in the authentication server 18 is requested as a certificate of a person permitted to distribute a program addressed to the UIM 12.

[1.4.4] Issue of certificate and distribution of program with certificate to UIM

[0049] The authentication server 18, upon receipt of a certificate issue request from the contents server 19, issues to the contents server 19 a UIM public key as a certificate corresponding to the UIM 12 specified by the particular issue request (step S14).

[0050] The contents server 19 encrypts the program of which distribution is requested, by use of the UIM public key corresponding to the UIM 12. The program obtained by the encryption is considered a program with a certificate for a legitimate person authorized to access the UIM 12.

[0051] Then, the program encrypted by the UIM public key is further encrypted by the contents server 19 using the distribution management server public key received from the authentication server 18 in advance. The program obtained by this encryption can be considered a program having attached thereto both a certificate showing a legitimate person authorized to access the UIM 12 and a certificate showing a legitimate person authorized to distribute a program through the distribution management server 16.

[1.4.5] Program distribution

[0052] The contents server 19 distributes the program obtained by the aforementioned two encryption sessions, to the distribution management server 16 through the network (step S15).

[0053] The distribution management server 16 decrypts the encrypted program distributed from the contents server 19, using the distribution management server private key. Once this decryption succeeds, the program encrypted only by the UIM public key can be obtained. In this case, the contents server 19 can be considered a legitimate person authorized to distribute a program addressed to the UIM 12. The distribution management server 16 transmits the data on the screen D2 shown in Fig. 7 to the mobile terminal 11, and causes the data to be displayed on the display section 21. This screen D2 is for making an inquiry at the user as to whether the program can be distributed or not.

[1.4.6] Writing in UIM

[0054] After the user confirms the screen D2 and performs the operation through the operating section 22 for permitting the program distribution, a notice to permit distribution is sent to the distribution management server 16. The distribution management server 16, upon receipt of the notice, distributes to the UIM 12 the program obtained by decryption, i.e. the program encrypted by the UIM public key (step S16).

[0055] This encrypted program is delivered as it is to the control unit 30 of the UIM 12 through the mobile terminal 11. Specifically, the mobile terminal 11 simply provides the UIM 12 with the communication function. This operation by the mobile terminal 11 guarantees the secure transmission to and the secure write operation into the UIM 12.

[0056] If the distribution management server 16 is to send a program to the UIM 12 in the aforementioned manner, it is necessary for the distribution management server 16 to establish a link with the UIM 12. This in turn requires the acquisition of the telephone number of the mobile terminal 11 with the UIM 12 connected thereto

or built therein.

[0057] In one conceivable method to achieve this, at the time of issuing a distribution request from the mobile terminal 11 to the contents server 19, the telephone number of the mobile terminal 11 is caused to be transmitted to the contents server 19 which sends this telephone number to the distribution management server 16. In this way, the distribution management server 16 can access the mobile terminal 11 using the telephone number sent to it, and thus can distribute the program addressed to the UIM 12.

[0058] Another available method is described below. Specifically, in advance of issuing a distribution request from the mobile terminal 11 to the contents server 19, an identifier is determined between the mobile terminal 11 and the distribution management server 16 in place of the telephone number of the mobile terminal 11, so that the distribution management server 16 stores the telephone number and the identifier as information corresponding to each other. The mobile terminal 11 sends a distribution request containing the identifier to the contents server 19, which in turn attaches the identifier to a program when sending the program to the distribution management server 16. The distribution management server 16 determines the telephone number of the mobile terminal 11 from the identifier, and based on this telephone number, calls the mobile terminal 11 and distributes the program addressed to the UIM 12. This method has the advantage that the need is eliminated of notifying the telephone number of the mobile terminal 11 to the contents server 19.

[0059] The control unit 30 of the UIM 12, upon receipt of a program encrypted by the UIM public key in the manner described above, decrypts the program using a UIM private key paired with the particular UIM public key. Once this decryption ends in success, a program is obtained in the form of an ordinary text not encrypted. In this case, the contents server 19 making up the origin is considered a person duly authorized to distribute a program to the UIM 12. The UIM 12 writes the program obtained by decryption, in the appropriate one of the basic blocks 40-1 to 40-6 of the memory.

[0060] During this write operation, the screen D3 shown in Fig. 7 is displayed by the mobile terminal 11.

[1.4.7] Write completion response

[0061] At the end of the program write operation, the control unit 30 of the UIM 12 transmits a write completion notice to the distribution management server 16 together with the information specifying the basic block having the particular program written therein (step S17).

[0062] In the process, the screen D4 indicating that the write operation is complete (the registration is over) is displayed, as shown in Fig. 7, on the display section 21 of the mobile terminal 11. After that, the screen is again turned to D1 by the user operation.

[1.4.8] Distribution completion notice

[0063] The distribution management server, upon receipt of a program write completion notice from the UIM 12, registers the information specifying the written program in a data base as information corresponding to the information indicating the basic block of the UIM 12 in which the particular program is written.

[0064] By accessing to the data base, the distribution management server 16 can easily grasp the program stored in each of all the basic blocks 40-1 to 40-6 of the UIM 12.

[0065] The distribution management server 16, upon distribution of a program into the UIM 12, starts the charge process against the contents provider of the contents server 19 from which the program is distributed. The timing of starting the charge process is not limited to this, but may be coincident with the timing of activation described later.

[0066] The contents provider are charged against the following items.

(a) Rental charge for basic blocks in UIM 12

[0067] Upon distribution of a program from the contents server 19 to the UIM 12, the particular program is stored in one of the basic blocks 40-1 to 40-6 in the UIM 12. The particular basic block can be considered to be rented to the contents provider owning the contents server 19 for storing the program. Thus, a charge corresponding to the rental period, i.e. the period during which the program is stored in the basic block is made against the contents provider as a rental charge.

(b) Transaction fee

[0068] The program transmitted from the contents server 19 is distributed to the UIM 12 through the process in the distribution management server 16. A consideration for the process performed by the distribution management server 16 is charged against the contents provider as a transaction fee.

[0069] The user of the UIM 12 receives the service in terms of the distribution of a program from the contents server 19, and therefore is required to pay the charge in consideration of the service. The distribution management server 16 may collect the service charge from the user on behalf of the contents provider together with the communication charge for the user, and delivers the collected service charge to the contents provider in the character of what might be called a "factor". In this case, the charge made against the contents provider may contain the factoring fee.

[0070] Upon complete program distribution, the distribution management server 16 notifies the contents server 19 (step S18).

[1.4.9] Activation

[0071] The program distributed to the UIM 12 and stored in the basic block cannot be executed by the user before activation.

[0072] The user only receives the distribution but is not permitted to execute the program distributed to him, in order to enable the contents provider to control the program execution start time.

[0073] The activation is effectively utilized, for example, in the case where the time to start the use of a newly marketed game program is determined. By use of the activation, the release date (program distribution date) and the date to start to use (activation date) can be set separately from each other, thereby making it possible to reduce the load on the contents server 19.

[0074] Another example is a case in which the program for using the mobile terminal 11 as a commutation pass is distributed to the UIM 12. In this case, the activation is utilized to make the program executable from the first date of the term of validity of the commutation pass.

[0075] The operation for activation will be explained below with reference to Fig. 8.

[1.4.9.1] Activation request to distribution management server

[0076] Whenever the activation becomes necessary for a given program, the contents server 19 sends an activation request to the distribution management server 16 (step S21). This activation request contains the information specifying a program to be activated. Also, in the case where only the program stored in the UIM 12 of a specific user is activated, the activation request contains the identifier (the telephone number of the mobile terminal 11 or an alternative identifier) of the particular user.

[1.4.9.2] Activation request to UIM

[0077] The distribution management server 16, upon receipt of an activation request, issues an activation request to the UIM 12 of the mobile terminal 11 (step S22). As already described, the information specifying the written program is registered in the data base of the distribution management server 16 as information corresponding to the information indicating the basic block of the UIM 12 in which the program is written. The distribution management server 16, upon receipt of the activation request, refers to the particular data base and determines the UIM 12 to which the program to be activated is distributed and the basic block in which the program is written. In the case where the same program stored in a plurality of UIMs 12 is activated, as many activation processes as the UIMs 12 are performed. Each mobile terminal 11 in which the corresponding UIM 12 is mounted or built is accessed, and an activation request is sent to the UIM 12. The activation request sent to each mobile terminal 11 contains the information specifying the basic block having stored therein the program to be activated.

[0078] This activation request, when received by the mobile terminal 11, is directly sent to the UIM 12. The control unit 30 of the UIM 12 executes the activation in accordance with the activation request. Specifically, the UIM 12 sets the activation flag from "0" to "1" for the basic block specified by the activation request. The control unit 30 of the UIM 12 responds to a request, if any, to execute the program stored in the basic block with the activation flag turned "1". A request, if any, to execute the program in the basic block with the activation flag "0", however, is rejected.

[1.4.9.3] Activation end response

[0079] The UIM 12, upon complete program activation, transmits an activation end notice to the distribution management server 16 (step S23). This notice contains the information specifying the program of which the activation is ended, or more specifically, the information specifying the basic block storing the particular program.

[1.4.9.4] Activation completion notice

[0080] The distribution management server 16, upon receipt of the activation completion notice from the UIM 12, determines the basic block of the UIM 12 in which the completely activated program is stored. The information to the effect that the activation is completed is registered in the storage area in the data base prepared for the particular basic block.

[0081] As the result of this registration, the distribution management server 16 can grasp, by accessing the data base, whether each program in the basic blocks 40-1 to 40-6 is activated or not for all the UIMs 12.

[0082] Upon registration of activation completion for all the UIMs to which the program of which the activation is requested are distributed, the distribution management server 16 notifies the contents server 19 that the program activation is complete (step S24). This notice contains the information specifying the program that has been activated.

[1.4.10] Deactivation

[0083] The program distributed to the UIM 12 and activated may require deactivation. This requirement occurs, for example, in a case where a program for the mobile terminal 11 to function as a credit card is stored in the UIM 12, and the user has lost the particular UIM 12. In such a case, the deactivation is started in response to the request from the user informed of the loss. Other examples include a case in which the user that has received a service has failed to pay the service

charge before the due date. In such a case, at the request of the contents provider providing such a service, the deactivation of the program for receiving the particular service can be started.

[0084] The deactivation process will be explained below with reference to Fig. 9.

[1.4.10.1] Deactivation request to distribution management server

[0085] The contents server 19, whenever required to deactivate a program distributed to a UIM 12, sends a deactivation request to the distribution management server 16 specifying the particular UIM 12 and the program to be deactivated (step S31).

[1.4.10.2] Deactivation request to UIM

[0086] The distribution management server 16, upon receipt of this deactivation request, accesses the data base and determines that basic block in the UIM 12 specified by the deactivation request which stores the program to be deactivated. Then, the distribution management server 16 sends a deactivation request to the mobile terminal 11 in which the particular UIM 12 is mounted or built (step S32). This deactivation request contains the information specifying the basic block storing the program to be deactivated.

[0087] The deactivation request is sent to the UIM 12 through the mobile terminal 11. The activation flag prepared for the basic block specified by the deactivation request is reset from "1" to "0" by the UIM 12. After that, the execution of the program in this particular basic block is prohibited.

[1.4.10.3] Deactivation end response

[0088] The UIM 12, upon termination of the program deactivation, notifies the distribution management server 16 (step S33). This notice contains the information specifying the program which has been deactivated, or specifically, the information specifying the basic block storing the program.

[1.4.10.4] Deactivation completion notice

[0089] The distribution management server 16, upon receipt of a program deactivation end notice from the UIM 12, determines, based on the notice, the basic block of the UIM 12 storing the program of which the deactivation has been completed. The information to the effect that the deactivation is complete is registered in the storage area of the data base prepared for the particular basic block.

[0090] Upon registration of completion of the deactivation, the distribution management server 16 notifies the contents server 19 of the completion of the deactivation (step S34).

[1.4.11] Deletion (only when desired by user)

[0091] A deactivated program wastefully occupies a memory area in the UIM 12. It is desirable for both the user and the contents provider to delete such an unnecessary program. The deletion of the program, however, cannot be left to the user. If the user arbitrarily deletes the program in the UIM 12, the rent charging process for the UIM would continue to proceed in spite of the program deletion, unless the fact of deletion is notified to the distribution management server 16 immediately.

[0092] According to this embodiment, therefore, whenever the user desires to delete a program, the program is deleted under the control of the distribution management server 16.

[0093] A deletion, based on a reason on the side of the contents provider, is basically not permitted due to the resulting complication of the charging process.

[0094] The operation of deleting a program in response to the desire of the user will be explained below with reference to Figs. 10 and 15.

[1.4.11.1] Program deletion request

[0095] The user accesses a predetermined home page of the contents provider by operating the operating section 22 of the mobile terminal 11. A distribution menu screen D11 shown in Fig. 15 is displayed on the display screen of the display section 21 of the mobile terminal 11. This distribution menu screen D11 is provided by the contents server 19 of the contents provider distributing the program. When the user selects a menu item meaning the deletion of a program, a screen D12 asking the user whether the deletion can be carried out is displayed on the display section 21 of the mobile terminal 11, as shown in Fig. 15.

[0096] The user performs the operation permitting the deletion. The mobile terminal 11 transmits a program (applet) deletion request to the contents server 19 through the network (step S41). This request contains the information specifying the program to be deleted.

[0097] With the transmission of a program deletion request, a screen D13 indicating that the deletion is going on, is displayed as shown in Fig. 15 on the display section 21 of the mobile terminal 11.

[1.4.11.2] Deactivation request to distribution management server

[0098] The contents server 19, upon receipt of a program deletion request, sends a deactivation request to the distribution management server 16 (step S42). This deactivation request contains the information specifying the mobile terminal 11 of the user requesting the program deletion and the information specifying the program to be deleted.

[1.4.11.3] Deactivation request to UIM

[0099] The distribution management server 16, upon receipt of a deactivation request, accesses the data-base and determines a basic block storing the program to be deleted. Then, the distribution management server 16 sends a deactivation request containing the information specifying the particular basic block to the mobile terminal 11 of the user requesting the program deletion (step S43).

[0100] This deactivation request is sent to the UIM 12 through the mobile terminal 11. The UIM 12resets, from "1" to "0" the activation flag prepared for the basic block specified by the deactivation request. After that, the execution of the program in the particular basic block is prohibited.

[1.4.11.4] Deactivation end response

[0101] The UIM 12, at the end of the program deactivation, transmits a deactivation end notice to the distribution management server 16 (step S44). This notice contains the information specifying the basic block storing the program deactivated.

[1.4.11.5] Deactivation end notice

[0102] The distribution management server 16, upon receipt of the program deactivation end notice from the UIM 12, registers the information to the effect that the deactivation is complete, in the area of the data base corresponding to the basic block of the UIM 12 specified by the deactivation end notice.

[0103] The distribution management server 16 sends a program deactivation end notice to the contents server 19 (step S45).

[1.4.11.6] Deletion request to distribution management server

[0104] The contents server 19, upon receipt of the deactivation end notice for the program to be deleted, from the distribution management server 16, requests the distribution management server 16 to delete the particular program (step S51).

[1.4.11.7] Deletion request to UIM

[0105] The distribution management server 16, upon receipt of the program deletion request, sends a program deletion request to the UIM 12 of the user who requests the program deletion (step S52). This program deletion request contains the information specifying the basic block storing the program to be deleted.

[0106] The program deletion request is sent to the UIM 12 through the mobile terminal 11. The UIM 12 deletes the program in the basic block specified by the program deletion request.

[1.4.11.8] Deletion end response

[0107] The UIM 12, at the end of the program deletion, transmits a deletion end notice indicating the program deletion to the distribution management server 16 (step S53). This deletion end notice contains the information specifying the basic block from which the program is deleted and the program deleted. At the same time, a screen D14 indicating the end of deletion is displayed, as shown in Fig. 15, on the display section 21 of the mobile terminal 11.

[1.4.11.9] Deletion completion notice

[0108] The distribution management server 16, upon receipt of the deletion end notice from the UIM 12, registers the information to the effect that the program has been deleted in the storage area in the data base corresponding to the combination of the user requesting the deletion and the program deleted.

[0109] Then, the distribution management server 16 sends to the contents server the notice that the program deletion is complete (step S54).

[0110] In the case where the charge process against the contents provider has been made for the program deleted, the distribution management server ceases to charge the contents provider thereafter.

[1.4.12] Deletion (only when desired by distribution management server)

[0111] According to this embodiment, a program may be deleted by other than the intention of the user. An example is the expiry of a predetermined term during which a program can be used.

[0112] The operation for deleting a program under the guidance of the distribution management server in such a case will be described below with reference to Fig. 11.

[1.4.12.1] Deactivation request to UIM

[0113] If the usable term of a program has expired and the program is required to be deleted, the distribution management server 16, by accessing the data base, determines all the UIMs 12 to which the program to be deleted has been distributed and the basic blocks storing the program to be deleted in each of the UIMs 12, and sends a deactivation request to each of the UIMs 12 (step S61). Each deactivation request contains the information specifying the basic block storing the program to be deleted.

[0114] The deactivation request is sent to each UIM 12 through the mobile terminal 11. The UIM 12 resets, from "1" to "0", the activation flag corresponding to the basic block specified by the deactivation request. After that, the execution of the program in the particular basic block is prohibited.

[1.4.12.2] Deactivation end response

[0115] At the end of the deactivation, the UIM 12 transmits a deactivation end notice to the distribution management server 16 (step S62).

[1.4.12.3] Deactivation completion notice

[0116] The distribution management server 16, upon receipt of the deactivation end notice from the party to which the program to be deleted has been distributed, registers the information indicating the completion of the deactivation in the storage area of the data base formed for the particular program.

[0117] The distribution management server 16 sends a program deactivation completion notice to the contents server 19 (step S63).

[1.4.12.4] Notification of deactivation completion notice receipt to distribution management server

[0118] The contents server 16, upon receipt of the deactivation completion notice from the distribution management server 16, sends a deactivation receipt notice to the distribution management server 16 (step S64).

[1.4.12.5] Deletion request to UIM

[0119] The distribution management server 16, upon receipt of the deactivation receipt notice, sends a program deletion request to the mobile terminal 11 that has transmitted the deactivation completion notice corresponding to the deactivation receipt notice (step S71). The deletion request sent to the mobile terminal 11 contains the information specifying the basic block storing the program to be deleted.

[0120] The UIM 12, upon receipt of the deletion request through the mobile terminal 11, deletes the program in the basic block specified by the request.

[1.4.12.6] Deletion end response

[0121] The UIM 12, at the end of the program deletion, transmits a deletion end notice to the distribution management server 16 (step S72). This notice contains the information specifying the basic block from which the program has been deleted.

[1.4.12.7] Deletion completion notice

[0122] The distribution management server 16, upon receipt of the deletion end notice from all the parties to which the program to be deleted has been distributed, registers the information to the effect that the program has been deleted, in the storage area of the data base formed for the particular program to be deleted.

[0123] The distribution management server 16 sends a deletion completion notice to the contents server 19 (step S73).

[0124] At the same time, the distribution management server ceases the charging process which may have hitherto been made against the contents provider for the deleted program.

[1.4.12.8] Deletion result receipt notice to distribution management server

[0125] The contents server 19, upon receipt of the deletion completion notice from the distribution management server 16, sends a deletion result receipt notice to the distribution management server 16 (step S74).

[1.4.13] Program distribution process for UIM version management

[0126] The contents server 19 may be required to distribute a program voluntarily regardless of the desire on the part of the user. An upgrade of the program that has been distributed is a case in point.

[0127] In such a case, the distribution of the program of a new version to the UIMs 12 of all the users to which the particular program has been distributed gives rise to an inconvenience. This is by reason of the fact that the mobile terminals 11 are of various models, and the UIM specifications have various versions. It may happen, therefore, that a program of a new version, if sent to all the UIMs, can be executed normally only by the UIMs having a version issued at a certain time point or thereafter.

[0128] According to this embodiment, at each time of an upgrade of a program, a version notice request is sent to the UIMs and based on the response to the request, it is determined whether the program is to be distributed or not to a given UIM. This operation is shown in Fig. 12. Some of the UIMs 12 support the function of notifying the version thereof in response to the version notice request, and others do not. Fig. 12 shows the operation performed in the case where a version notice request has been sent to a UIM supporting such a function and the operation performed in the case where a version notice request has been sent to a UIM not supporting the function.

[1.4.13.1] Operation for UIM supporting version notice function

[1.4.13.1.1] Program distribution request to distribution management server

[0129] Prior to distribution of a program after upgrade, the contents server 19 sends to the distribution management server 16 a program distribution request containing the information specifying the program and the version information indicating the version of the UIM 12 that can execute the particular program (step S81).

[1.4.13.1.2] Version notice request to UIM

[0130] The distribution management server 16, upon receipt of the program distribution request, accesses the data base, determines all the mobile terminals 11 to which the program specified by the program distribution request has been distributed, and sends a version notice request to the mobile terminals 11 thus determined (step S82).

[1.4.13.1.3] Version notice

[0131] The version notice request is sent to each UIM 12 through the mobile terminal 11. The UIM 12, upon receipt of the version notice request, notifies the version thereof to the distribution management server 16 (step S83).

[1.4.13.1.4] No program distribution notice

[0132] The distribution management server 16 receives a version notice from each UIM 12. In the case where the version notice received from a given UIM 12 fails to meet the conditions indicated by the version information from the contents server 19, the contents server 19 is notified that the program cannot be distributed to the particular UIM 12 (step S84).

[0133] In the case where the version notice received from another given UIM 12 meets the conditions indicated by the version information from the contents server 19, on the other hand, the distribution management server 16 distributes the program to the particular UIM 12. This operation is described above with reference to Figs. 6 and 8.

[1.4.13.2] Operation for UIM not supporting version notice function

[1.4.13.2.1] Program distribution request to distribution management server

[0134] The contents server 19 sends a program distribution request to the distribution management server 16 in the same manner as described above (step S91).

[1.4.13.2.2] Version notice request to UIM

[0135] The distribution management server 16 sends a version notice request to the UIM 12 of the mobile terminal 11 (step S92).

[1.4.13.2.3] Timer count

[0136] In this case, the UIM 12 does not support the version notice function, and therefore makes no response.

[0137] Thus, the distribution management server 16 monitors the timer, and upon expiry of a predetermined time-out period (step S93), sends a version notice request again to the UIM 12 of the mobile terminal 11 (step S94). Then, the value on the retry counter is incremented by one.

[0138] In a similar fashion, the distribution management server 16 monitors the timer, and upon expiry of a predetermined time-out period (step S95), sends a version notice request again to the UIM 12 of the mobile terminal 11 (step S96). Then, the value of the retry counter is incremented by one.

[1.4.13.2.4] No program distribution notice

[0139] Once again, the distribution management server 16 monitors the timer, and upon expiry of a predetermined time-out period (step S97), sends a version notice request again to the UIM 12 of the mobile terminal 11 (step S98). Then, the value on the retry counter is incremented by one.

[0140] In the case where the figure on the retry counter reaches a predetermined value (3 in this case), the distribution management server 16 determines that the version of the UIM 12 fails to meet the conditions for the version notified from the contents server 19, and sends a no-program distribution notice to the contents server 19 (step S84).

[0141] As a result, the contents server 19 confirms that the program of which distribution is desired, cannot be distributed.

[1.4.14] Program distribution process based on UIM memory capacity limitation

[0142] The limitation of the memory capacity of the UIM 12 may make the program distribution impossible, even if desired by the contents server 19. An example of the operation performed in such a case is shown in Fig. 13. This operation will be explained below.

[1.4.14.1] Rejection by distribution management server

[0143] The contents server 19 requests the distribution management server 16, by attaching the program to be distributed, to send a program distribution request to the UIM 12 (step S101).

[0144] The information indicating the memory state of each UIM is registered in the database of the distribution management server 16. The distribution management server 16, upon receipt of the program distribution request to a given UIM 12, accesses the data base, and determines whether the basic block for the particular UIM 12 is available for storage, or if available, is too small in capacity to store the program (the capacity may vary from one version to another of UIM) or whether there is any other stumbling block to the program distribution.

[0145] In the case where the program cannot be distributed, the distribution management server 16 sends

a notice to the contents server 19 that the program cannot be distributed due to the shortage of the memory capacity (step S102).

[0146] As a result, the contents server 19 confirms that the program for which distribution is desired, cannot be distributed.

[1.4.14.2] Rejection by UIM

[0147] The memory capacity and the current occupancy state of each UIM 12 are registered in the database of the distribution management server 16. For some reason or other, however, the actual UIM memory state may differ from the memory state registered in the database of the distribution management server 16. The operation performed in such a case is described below.

[0148] First, the contents server 19 sends a program distribution request together with a program to the distribution management server 16 (step S111).

[0149] The distribution management server 16 accesses the data base and determines whether the basic block of the destination UIM 12 is available for storage and has a sufficient capacity.

[0150] In the case where the determination is YES, the distribution management server 16 sends a write request together with the program to the UIM 12 (step S112).

[0151] The UIM 12 that has received the write request determines whether the program attached to the write request can be stored in any one of the basic blocks or not. In the case where the determination is NO, the UIM 12 sends a no-program distribution notice to the distribution management server 16 due to lack of memory capacity (step S113).

[0152] The distribution management server 16, upon receipt of the no-program distribution notice due to lack of memory capacity, sends it to the contents server 19 (step S114).

[0153] From this notice, the contents server 19 can confirm that the program cannot be distributed to the UIM to which the distribution is desired.

[0154] It may also happen that a program cannot be stored in a basic block due to a write error in the memory of the UIM 12 or the malfunction of the memory device. In such a case, exactly the same operation as described above is performed. Fig. 14 shows such an operation. In Fig. 14, steps S121 to S124 correspond to steps S111 to S114 in Fig. 13 and represent exactly the same operation, respectively.

[1.4.15] Specific example of operation

[0155] Now, a specific example of the operation according to this embodiment will be explained.

[1.4.15.1] Execution of program stored in UIM

[0156] In this example of an operation, assume that a program called " ○ ○ RAILWAY" is stored in the basic block 40-1 of the UIM 12.

[0157] The user operates the operating section 22 of the mobile terminal 11 and thus accesses the home page of the contents provider that has distributed the "○○ RAILWAY" program. A distribution menu screen D21 as shown in Fig. 16 is displayed on the display screen of the display section 21. This distribution menu screen D21 is provided by the contents server 19 of the contents provider. The user performs the operation for selecting an item concerning the purchase of a commutation pass from the menu displayed on the distribution menu screen D21. A purchase request for the commutation pass is transmitted from the mobile terminal 11 to the contents server 19 through the network.

[0158] As a result, a download screen D22 is sent from the contents server 19 to the mobile terminal 11 and displayed on the display section 21. The download screen D22 contains a menu of several value data having the same monetary value as the commutation pass.

[0159] Once the user selects the desired value data, the information requesting the selected value data is sent to the contents server 19 from the mobile terminal 11.

[0160] After that, the contents server 19 sends to the mobile terminal 11 the screen data for selecting a method of account settlement. As a result, a screen D23 is displayed by the mobile terminal 11. The user selects "SELECT FROM UIM MENU" from the menu items in the screen D23, and thus can settle the account by use of the program in the UIM 12. Specifically, once this select operation is performed, the UIM 12 is notified of the fact. Upon receipt of this notice, the control unit of the UIM 12 returns to the mobile terminal 11 the list of the programs stored in the basic blocks 40-1 to 40-6. The screen D24 containing this list is displayed on the display section 21 of the mobile terminal 11. The user selects a settlement program from the list. The selected program is executed by the UIM 12 thereby to settle the account.

[0161] Assume that the account is settled by executing the program in the program area 41 of the basic block 40-2. The data area 42 of the same basic block 40-2 is used for settling the account.

[0162] The contents server 19, upon detection that the account has been settled, sends the value data of the commutation pass included in the commutation pass purchase request described above, to the mobile terminal 11. This value data contains the information such as the names of the two stations involved, the validity term, the name of the user and the age of the user and are sent from the mobile terminal 11 to the UIM 12. The value data, which are to be used for the "○○ RAILWAY" program, are stored in the data area 42 of the basic block 40-1 corresponding to the same data in the UIM 12.

[1.4.15.2] Mail order sale using network

[0163] In this example of an operation, a program for a mail order sale is stored in the basic block 40-2 of the UIM 12.

[0164] The user accesses the home page of the contents provider by operating the operating section 22 of the mobile terminal 11, so that a distribution menu screen D31 shown in Fig. 17 is displayed on the display section 21 of the mobile terminal 11. This distribution menu screen D31 is provided by the contents server 19 of the contents provider which in turn provides the mail order sale (what is called "e-commerce") service utilizing the network. The user selects the desired commodity (MATSUZAKA BEEF FOR SUKIYAKI, Y5000/KG, in Fig. 17) from the commodities listed in the distribution menu screen D31. Then, a purchase request is transmitted from the mobile terminal 11 to the contents server 19 through the network.

[0165] The contents server 19 that has received the purchase request returns a settlement method screen D32 to the mobile terminal 11. As a result, a select screen D32 is displayed on the display section 21.

[0166] From the settlement methods listed in the select screen D32, the user is assumed to have selected "XX BANK". The settlement program for XX Bank stored in the basic block 40-3 of the UIM 12 is started by the control unit 30 of the UIM 12 and a settlement screen D34 is displayed.

[0167] The user inputs the personal identification (ID) number as settlement information. The mobile terminal 11 tries to connect the settlement server for XX Bank through a communication unit 34 and the network, so that the screen D35 being accessed is displayed.

[0168] Upon complete authentication, a purchase amount confirmation screen D36 is displayed.

[0169] The user confirms the amount to be paid and inputs the confirmation. The mobile terminal 11 displays a payment confirmation screen D37 of the contents provider, i.e. the mail order house, together with the delivery date, etc.

[1.4.15.3] Use of commutation pass (check gate passage, manual start)

[0170] According to this embodiment, the mobile terminal 11 can be used as a commutation pass by storing an appropriate program in the UIM 12. An example of operation will be explained below.

[0171] First, the user depresses a button 23. A UIM menu screen D41 shown in Fig. 18 is displayed on the display section 21. The user selects "○○ RAILWAY" for which the commutation pass is used. As a result, the control unit 30 of the UIM 12 executes the ○○ RAILWAY program in the basic block 40-1, so that a menu screen D42 is displayed on the display section 21.

[0172] When the screen D42 is displayed, the user selects "4. SET APPLICATION AUTO. START". An automatic start set confirm screen D43 is displayed thereby prompting the user to select.

[0173] In the case where the user selects "YES", the automatic start is set. In the case where the user selection is "NO", on the other hand, the automatic start is not set.

[0174] The gate of the railway company is equipped with a ticket check reader/writer. Before passing through the gate, the user performs the following operation.

[0175] First, the user depresses the U button 23. The UIM menu screen D41 shown in Fig. 19 is displayed on the display section 21. The user then selects " ○○ RAILWAY" for which the pass is used. As a result, the control unit 30 of the UIM 12 executes the ○○ RAILWAY program in the basic block 40-1, and displays the menu screen D42 on the display section 21. The user selects " 1. PASS". The pass program constituting a part of the ○○ RAILWAY program is started by the control unit 30. In accordance with this pass program, the control unit 30 begins communication with the ticket reader/writer for pass check. In the case where this communication is carried out by the common key cryptosystem, for example, the pass check process is performed following the steps described below.

(1) Each party checks the other party.
(2) The ticket check reader/writer requests the mobile terminal 11 to transmit information on the commutation pass.
(3) The mobile terminal 11 encrypts the pass information by the common key and transmits it to the ticket check reader/writer. The pass information display screen D53 is displayed on the display section of the mobile terminal 11.
(4) The ticket check reader/writer decrypts the received commutation pass information, and, in the case where the user is found to be legitimate, the gate is opened to allow him in.

[0176] At the same time, a message screen D54 for expressing gratitude to the user is displayed on the display section 21.

[0177] The foregoing description deals with the commutation pass. In the case where the mobile terminal 11 is used to function as a private card, however, the data area 42 is updated to indicate the value data corresponding to the amount after subtracting the actual charge in the process of (4) above.

[1.4.15.4] Use of commutation pass (gate passage: auto. start)

[0178] When the screen D43 shown in Fig. 18 is displayed, the user can select "YES" and the automatic start is set. The following operation is performed. Specifically, when the mobile terminal 11 set to the automatic start mode approaches the gate of the station, a polling signal transmitted from the ticket check reader/writer

is received by the mobile terminal 11. As a result, the pass program constituting a part of the ○○ RAILWAY program is automatically started by the control unit 30 in the UIM 12, and the pass check similar to the manual start is carried out.

[1.5] Effect of first embodiment

[0179] As described above, according to this embodiment, even in the case where the storage area of the storage module is divided to store each program, the mobile terminal simply provides the communication function to the UIM, and no extra burden is imposed on the mobile terminal. Therefore, the inherent function of the mobile terminal is not adversely affected

[0180] Also, the program storage, the activation, the deactivation and the deletion are not carried out by the mobile terminal, but under the control of the distribution management server. Thus, the user convenience is improved while at the same time maintaining security.

[2] Second embodiment

[0181] According to the first embodiment described above, the program executed by the UIM 12 is stored in the basic blocks 40-1 to 40-6 in the same UIM. In the second embodiment, however, all the programs executed are not necessarily stored in the basic blocks.

[2.1] Configuration of second embodiment

[0182] Fig. 21 is a block diagram showing a configuration of a program distribution system according to a second embodiment of the invention.

[0183] A UIM 12, contents servers 19-1 to 19-6 and 19X and a distribution management server 16A are shown in Fig. 21. The distribution management server 16A corresponds to the distribution management server 16 of the first embodiment plus the functions unique to this embodiment. The contents servers 19-1 to 19-6 and 19X have similar functions to the contents server 19 of the first embodiment. The system according to this embodiment has an authentication server, as in the first embodiment, not shown in Fig. 21.

[0184] The UIM 12 according to this embodiment includes an application area 12C shown in Fig. 22 in place of the application area 12B of the first embodiment. The program storage area 12C is divided into seven basic blocks 40-1 to 40-7 and one free basic block 40-1.

[0185] The basic blocks 40-1 to 40-7 and the free basic block 40-F1 each have a program area 41 and a data area 42. A program (application or applet) is stored in the program area 41. The data area 42, on the other hand, has stored therein the data used by the program stored in the program area 41 of the same basic block or the free basic block.

[0186] In this case, the basic blocks 40-1 to 40-7 and the free basic block 40-F1 are independent of each other, and basically, the program stored in the program area 41 of a given block cannot access the data area 42 of other blocks. This is also the case with the first embodiment. The program stored in the program area 41 cannot be distributed or deleted without intermediary of the distribution management server 16A. The data area 42, however, can be directly operated through the distribution management server 16A or a local terminal as in the case where electronic money is downloaded from the ATM. This point is also similar to the first embodiment.

[0187] According to this embodiment, the distribution of the programs stored in the basic blocks 40-1 to 40-7 is controlled by the distribution management server 16A. The program stored in the free basic block 40-F1, however, is controlled not by the distribution management server 16A but on the user's own responsibility.

[0188] According to the first embodiment, the program transmitted from the contents server 19, in accordance with the distribution request from the mobile terminal 11, is sent to the UIM 12 by the distribution management server 16. The distribution management server 16A according to this embodiment, on the other hand, accepts the program distribution request from the mobile terminal 11, and on acquiring the program by accessing the contents server as required, distributes it to the UIM 12 of the mobile terminal 11. The distribution management server 16A according to this embodiment is similar to the distribution management server 16 of the first embodiment in that the program distribution from the contents server to the UIM 12 is relayed and managed. This operation, however, is not the only function of the distribution management server 16A according to this embodiment. Specifically, the distribution management server 16A has means for storing a program or the information indicating the location of the program for the benefit of the user of the UIM 12, and any of the programs stored in this means can be acquired by the user through the distribution management server 16A. In this sense, the distribution management server 16A exhibits a function similar to a cache memory for the UIM 12.

[0189] In order to manage the program distribution to the UIM 12 and exhibit the function like a cache memory, the distribution management server 16A includes a distribution management unit 50. The distribution management unit 50 has a user information storage unit 51 and a program information storage unit 52.

[0190] The program information storage unit 52 has stored therein a program proper or a URL corresponding to the program that can be distributed to the UIM 12. The URL is the information indicating the address of a specific one of the contents servers 19-1 to 19-6 and the very contents server where a particular program is located. Which is to be stored in the program information storage unit 52 for a given program, the URL information or the program proper, can be determined based on the storage capacity of the program information storage unit

52, or in the case where the storage capacity is sufficient, can be selected as desired by the contents provider operating the distribution server.

[0191] The chance of storing a new program or the URL thereof in the program information storage unit 52 is given, for example, in the case where the mobile terminal 11 of a given user sends a program distribution request, and a program or the URL thereof meeting the particular distribution request is not stored in the program information storage unit 52. In such a case, the program information storage unit 52 accesses the contents server and acquires and stores the program desired by the user, in compliance with the request from the mobile terminal 11.

[0192] The user information storage unit 51 includes n (n > 1) individual user information storage units 53-1 to 53-n corresponding to n persons to which the system, according to the invention, is applicable. Each individual user information storage unit 53-k has a real distribution information storage unit 54 and a virtual distribution information storage unit 55.

[0193] The real distribution information storage unit 54 of the individual user information storage unit 53-k has stored therein pointer data corresponding to the program actually distributed to the UIM 12 of the user k. The pointer data is for indicating a particular area in the program information storage unit 52 where the program or the URL thereof is stored. The availability of the real distribution information storage unit 54 makes it possible for the distribution management server 16A to immediately redistribute any program, if erased, in the basic blocks 40-1 to 40-7 of the UIM 12.

[0194] The virtual distribution information storage unit 55 of the individual user information storage unit 53-k, on the other hand, stores the pointer data corresponding to an available program, though not actually distributed to the UIM 12 of the user k, that can be immediately distributed to the UIM 12 of the user k who is desirous of having such a program. The user of the UIM 12 can receive the following services by use of the virtual distribution information storage unit 55.

(a) The pointer data of a program of which distribution to the UIM 12 is desired is provisionally stored in the virtual distribution information storage unit 55. The user, whenever the distribution of the program with the pointer data thereof stored in the virtual distribution information storage unit 55 is required, sends a request to the distribution management server 16A using the mobile terminal 11. The distribution management server 16A reads the pointer data of the requested program from the virtual distribution information storage unit 55, and acquires and distributes the program specified by the particular pointer data to the UIM 12. In this case, the pointer data of the program distributed to the UIM 12 is moved from the virtual distribution information storage unit 55 to the real distribution information storage unit 54.

(b) The number of the basic blocks in the UIM 12 is limited. Therefore, it may happen that all the basic blocks are occupied and no basic block is available for storing the program to be distributed. In such a case, the distribution management server 16A reads the pointer data from the storage area corresponding to a given basic block 40-X in the UIM 12, from among the storage areas in the real distribution information storage unit 54, and transfers it to the virtual distribution information storage unit 55. The program to be distributed is sent to the UIM 12, where it is written in the basic block 40-X, and the pointer data of the program is written in the storage area corresponding to the basic block 40-X in the real distribution information storage unit 54. This process makes it possible to acquire a program by a distribution request and store it in a basic block even in the case where the basic blocks are fully occupied. In the process, with regard to the program driven away from the basic block, a request may be given again, if required, to the distribution management server 16A and the process described in (a) above can be carried out.

[0195] Now, an explanation will be given of the function of the distribution management server 16A corresponding to the free basic block 40-F1. As already described, as for the free basic block 40-F1, the distribution management server 16 does not manage the program distribution. The user, by operating the mobile terminal 11, can freely register or delete a program in the free basic block 40-F1.

[0196] The real distribution information storage unit 54 of the individual user information storage unit 53 has a storage area corresponding to the basic block 40-F1 of the UIM 12. In this area, however, no pointer data of a program is stored, but the data including the number of times a program is registered in or deleted from the basic block 40-F1 or the URL information thereof. In the case where nothing is stored in the free basic block 40-F1, the data indicating the fact ("Null" data, etc.) may be stored in this area.

[0197] The program in the free basic block 40-F1 of the UIM 12, should it be deleted, unlike the programs stored in the basic blocks 40-1 to 40-7, remains as it is until registered again by the user himself.

[0198] In the case where the user is desirous of changing the program in the free basic block 40-F1 temporarily to another program, on the other hand, such a change can be made always by the user himself rewriting it.

[0199] In such a case, the distribution management server 16A cannot carry out the charging process even if a program is stored in the free basic block 40-F1.

[0200] The free basic block 40-F1 can be changed so that it can be handled the same way as the basic blocks 40-1 to 40-7 as desired by the user. Specifically, before

the change, seven basic blocks 40-1 to 40-7 and one free basic block 40-F1 can be used as eight basic blocks 40-1 to 40-8.

[0201] In such a case, the information to the effect that the free basic block 40-F1 has been changed to the basic block 40-8 is written by the distribution management server 16A in the system area 12A (Fig. 4) of the UIM 12. Also, the area in the real distribution information storage unit 54 that has hitherto been handled as an area corresponding to the free basic block 40-F1 can be handled by the distribution management server 16A as an area corresponding to the basic block 40-8, and using this area, the same management as that of the basic blocks 40-1 to 40-7 is started.

[0202] The basic block that has been changed to the basic block 40-8 by the user in this way can be restored to the free basic block 40-F1 again. The basic blocks 40-1 to 40-7 cannot be changed to free basic blocks.

[2.2] Configuration of distribution management server

[0203] A configuration of the distribution management server is shown in Fig. 23.

[0204] The distribution management server 16A is roughly configured of a transmission control unit 61, the user information storage unit 51 described above, the program information storage unit 52 described above and a secure communication control unit 62.

[0205] The transmission control unit 61 controls the transmission between the external contents servers 19-1 to 19-6 or between the mobile terminals 11 (including the transmission between the contents servers 19-1 to 19-6 and the mobile terminals 11). The transmission control unit 61 also controls the transmission between the user information storage unit 51, the program information storage unit 52 and the secure communication control unit 63 to each other. Further, the transmission control unit 61 controls the distribution management unit 50, the user information storage unit 51, the program information storage unit 52 and the secure communication control unit 63 on the one hand, and requests the execution of various processes in the distribution management unit 50, the user information storage unit 51, the program information storage unit 52 and the secure communication control unit 63 on the other hand.

[0206] The program information storage unit 52 substantially functions as a portal site for the program permitted to be distributed to the basic blocks 40-1 to 40-7 of the UIM 12.

[0207] The secure communication control unit 63 authenticates the information (an encrypted program, etc.) sent from the contents servers 19-1 to 19-6, holds the public key paired with the private key held by each UIM, and manages the issue of the public keys for the contents servers 19-1 to 19-6.

[2.3] Operation of second embodiment

[2.3.1] Registration in user information storage unit

[0208] In the example shown in Fig. 21, the contents servers 19-1 to 19-6 are under the control of the distribution management server 16A. The user desirous of using a program (applet) stored in any of the contents servers is required to register the particular program in the user information storage unit 51 of the distribution management server 16A. The registration process will be explained below with reference to Fig. 24.

[0209] First, the user sends a request for a menu list of the programs that can be registered, to the distribution management server 16A from the mobile terminal 11. This request is sent to the program information storage unit 52 through the transmission control unit 61 of the distribution management server 16A (step S131).

[0210] The program information storage unit 52 that has received the request prepares a menu list of all the programs that can be registered or, specifically, all the programs of which the program proper or the URL is stored in the program information storage unit 52, and transmits the menu list through the transmission control unit 61 to the mobile terminal 11 (step S132).

[0211] This menu list is received by the mobile terminal 11 and displayed on the display section 21. Under this condition, the user can acquire, by operating the operating section 22, a comment on the desired program from the distribution management server 16A and display it on the display section 21.

[0212] Once the program of which distribution is requested is determined by the user operating the operating section 22, the mobile terminal 11 transmits a registration request containing the information specifying the particular program to the program information storage unit 52 of the distribution management server 16A (step S133).

[0213] The program information storage unit 52, based on the program registration request, registers the program requested by the user in the user information storage unit 51 (step S134).

[0214] The operation in step S134 will be described in detail. First, assume that the registration request is issued from the mobile unit 11 in which the UIM 12 of a given user k is built or mounted. In this case, the program information storage unit 52, based on the registration request, identifies the program requested by the user, and determines the pointer data for specifying the internal area of the program information storage unit 52 in which the URL information indicating the location of the program or the program proper thereof is stored. Once the pointer data of the program requested by the user is obtained in this way, the program information storage unit 52 accesses the contents stored in each area of the real distribution information storage unit 54 of the individual user information storage unit 53-k corresponding to the user k, and thus determines the basic

block 40-X ($1 \leqq X \leqq 7$) available for storage among the basic blocks of the UIM 12 of the user k. The pointer data of the program requested by the user is registered in the area of the real distribution information storage unit 54 corresponding to the basic block 40-X (step S134). It may be that the UIM 12 of the user k has no basic block 40-X ($1 \leqq X \leqq 7$) available for storage. In such a case, the program information storage unit 52 registers the pointer data in the virtual distribution information storage unit 55 designated by the user or set automatically.

[0215] In step S141, the menu list may not have any desired program. In such a case, the user can request the program information storage unit 54, by operating the mobile terminal 11, to access to the desired contents server. In this case, the program information storage unit 54, in compliance with the user request, acquires the program or the URL thereof from the contents server desired by the user, and holds it in the unoccupied area in the program information storage unit 54. In the process, the pointer data indicating the location of the acquired program or the URL thereof is registered in the real distribution information storage unit 54 in the same manner as the procedure mentioned above.

[0216] Upon complete registration of the program requested by the user in this way, the distribution management server 16A starts the charge process for the user or the contents provider that has distributed the particular program.

[0217] Then, the user information storage unit 51 sends a registration notice to the mobile terminal 11 through the transmission control unit 61 (step S135).

[0218] The mobile terminal 11, upon receipt of the registration notice, sends a registration acknowledgment to the distribution management server 16A (step S136).

[0219] The user information storage unit 51, upon receipt of the registration acknowledgment through the transmission control unit 61 from the mobile terminal 11 having the UIM 12 of the user k built therein or connected therewith, determines the contents provider 19 storing the program of which the pointer data has been registered for the user k, and sends an activation permission request to the contents server 19 (step S137).

[0220] The contents server 19 that has received the activation permission request, in order to approve a program utilization contract, sends the activation permission to the user information storage unit 51 (step S138). As a result, the user information storage unit 51 considers that the use is permitted of the pointer data stored in that area of the real distribution information storage unit 54 of the individual user information storage area 53-k for the user k which corresponds to the basic block 40-X.

[0221] The user information storage unit 51 sends a registration completion notice indicating that the registration in the mobile terminal 11 is completed (step S139). This registration completion notice contains a registration list providing a list of the programs with the pointer data thereof registered in the user information storage unit 51.

[0222] The user can confirm the registration list from the display section 21 of the mobile terminal 11.

[2.3.1.1] Registration of UIM in basic block (the contents server holding the program)

[0223] The user k who has received the registration list can request the program for which he has requested registration, to be distributed and written in the UIM 12. With reference to Fig. 25, this operation will be explained.

[0224] The user k performs the operation for selecting a program of which distribution is desired from the registration list. Then, a distribution request containing the pointer in the registration list, indicating the position number in the registration list where the particular program is located, is sent to the user information storage unit 51 of the distribution management server 16A from the distribution terminal 11 (step S141).

[0225] The user information storage unit 51, upon receipt of a distribution request from the mobile terminal 11 of the user k, reads the pointer data specifying the place of storing the program proper or the URL of the program requiring distribution, from that area of the real distribution information storage unit 54 of the individual user information storage unit 53-k which corresponds to the pointer in the registration list contained in the particular distribution request. The distribution request containing the pointer data is sent to the program information storage unit 52 (step S142).

[0226] The program information storage unit 52 accesses the area specified by the pointer data in the particular distribution request. In the case where the URL of the program is stored in the area, the program distribution is requested from the contents server 19 using the URL (step S143).

[0227] The contents server 19, upon receipt of this distribution request, requests the authentication server 18 to issue a public key for the distribution management server (step S144).

[0228] In the case where the contents server 18 is permitted to write in the UIM 12, the authentication server 18 issues the public key for the distribution management server to the contents server 19 (step S145).

[0229] The contents server 19 encrypts the program using the public key for the distribution management server, and distributes it as a program, with a certificate, to the secure communication control unit 62 of the distribution management server 16A (step S146).

[0230] The secure communication control unit 62 has stored therein a distribution management server private key paired with the distribution management server public key, and using this private key, decrypts the program with a certificate. In the case where this decryption is successful, a program written in a common text is obtained.